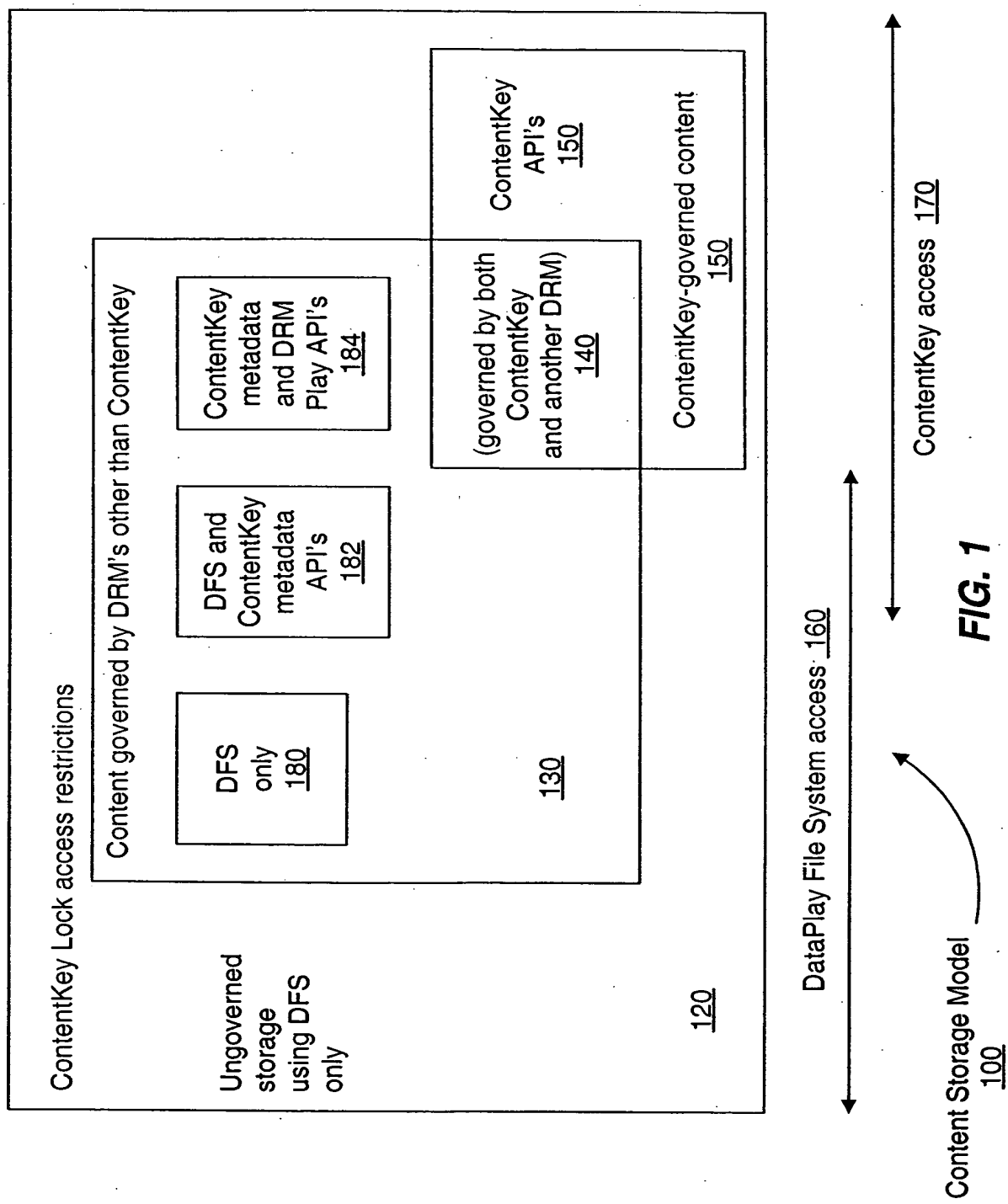

ContentKey Lock access restrictions
Ungoverned storage using DFS only
120
Content governed by DRM's other than ContentKey
130
DFS only 180
DFS and ContentKey metadata API's 182
ContentKey metadata and DRM Play API's 184
(governed by both ContentKey and another DRM) 140
ContentKey-governed content 150
ContentKey API's 150
DataPlay File System access 160
ContentKey access 170
Content Storage Model 100

FIG. 1

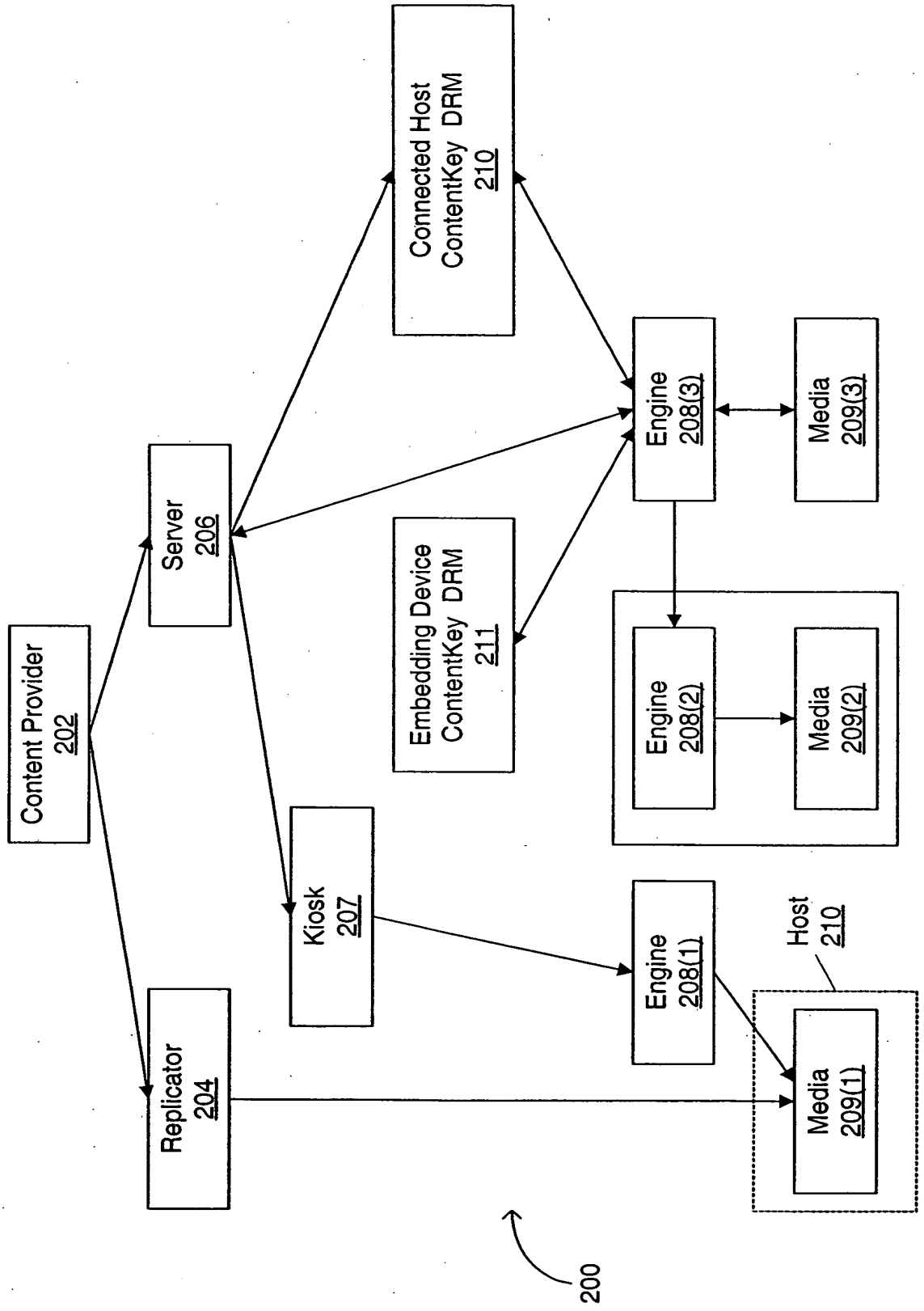

Content Provider 202
Server 206
Connected Host ContentKey DRM 210
Embedding Device ContentKey DRM 211
Engine 208(3)
Media 209(3)
Engine 208(2)
Media 209(2)
Kiosk 207
Engine 208(1)
Host 210
Media 209(1)
Replicator 204
200

FIG. 2

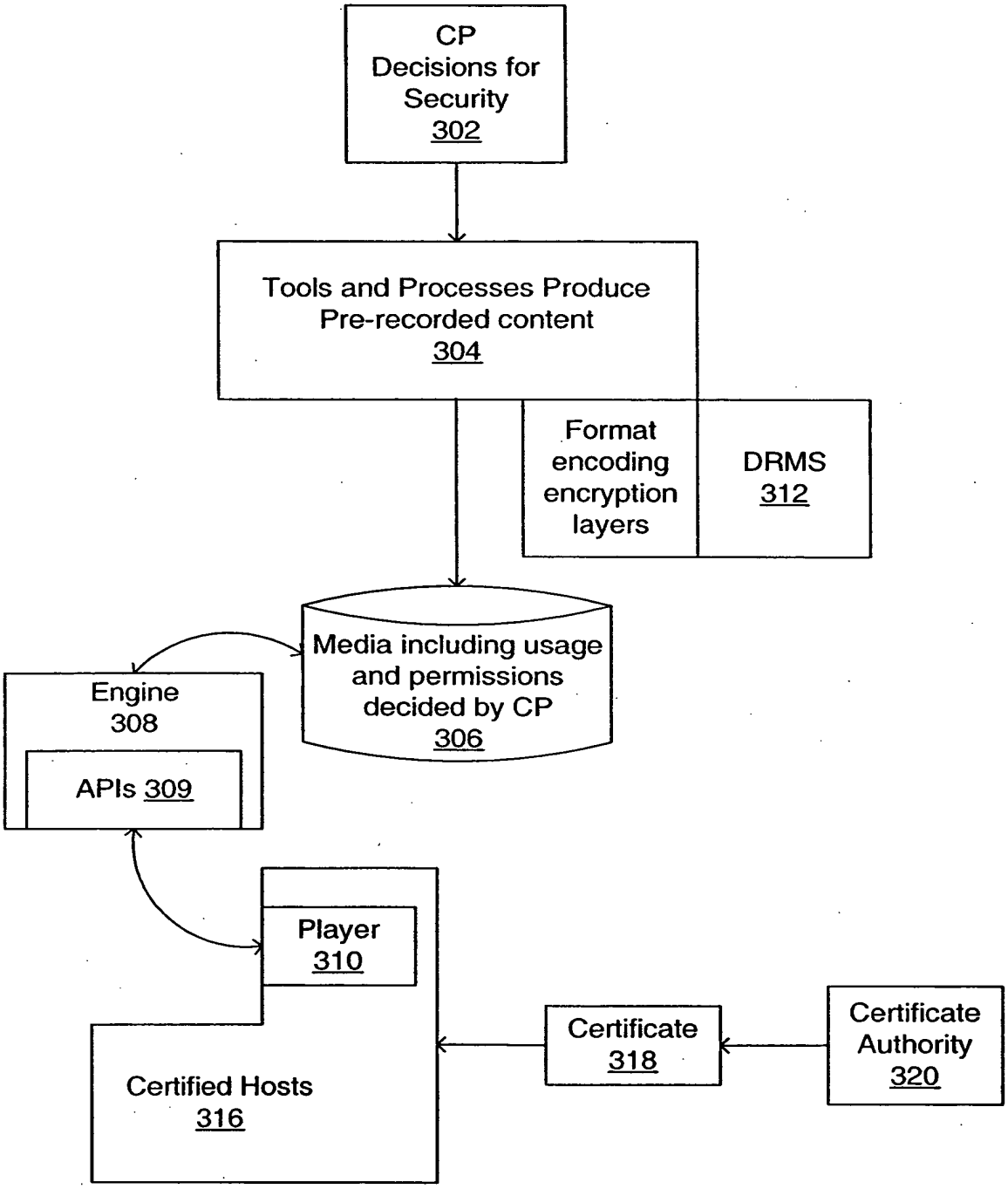


FIG. 3

Docket #M-12041 US

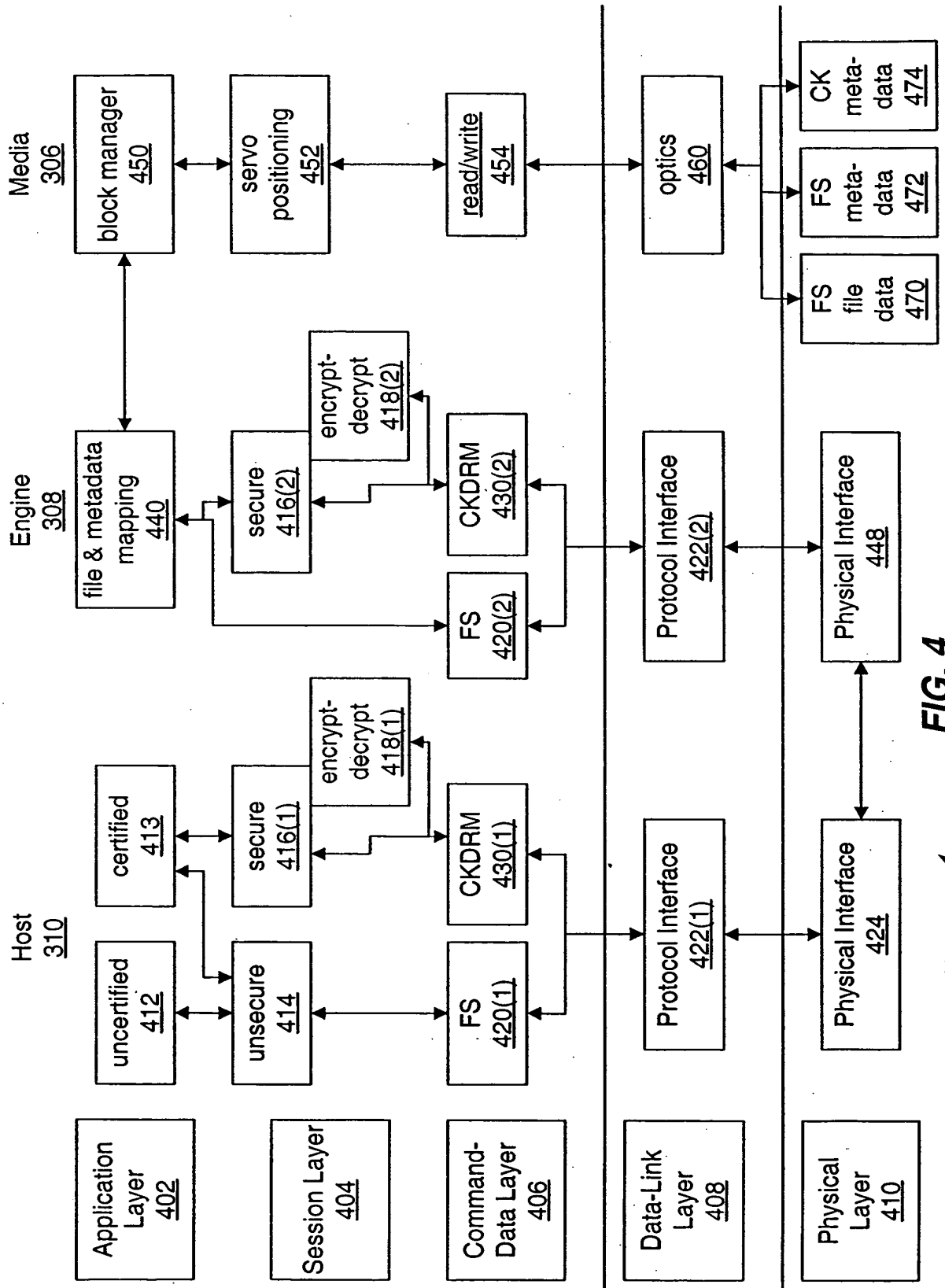

Application Layer 402
Session Layer 404
Command-Data Layer 406
Data-Link Layer 408
Physical Layer 410
Host 310
uncertified 412
certified 413
unsecure 414
secure 416(1)
encrypt-decrypt 418(1)
FS 420(1)
CKDRM 430(1)
Protocol Interface 422(1)
Physical Interface 424
Engine 308
file & metadata mapping 440
secure 416(2)
encrypt-decrypt 418(2)
FS 420(2)
CKDRM 430(2)
Protocol Interface 422(2)
Physical Interface 448
Media 306
block manager 450
servo positioning 452
read/write 454
optics 460
FS file data 470
FS meta-data 472
CK meta-data 474
400

FIG. 4

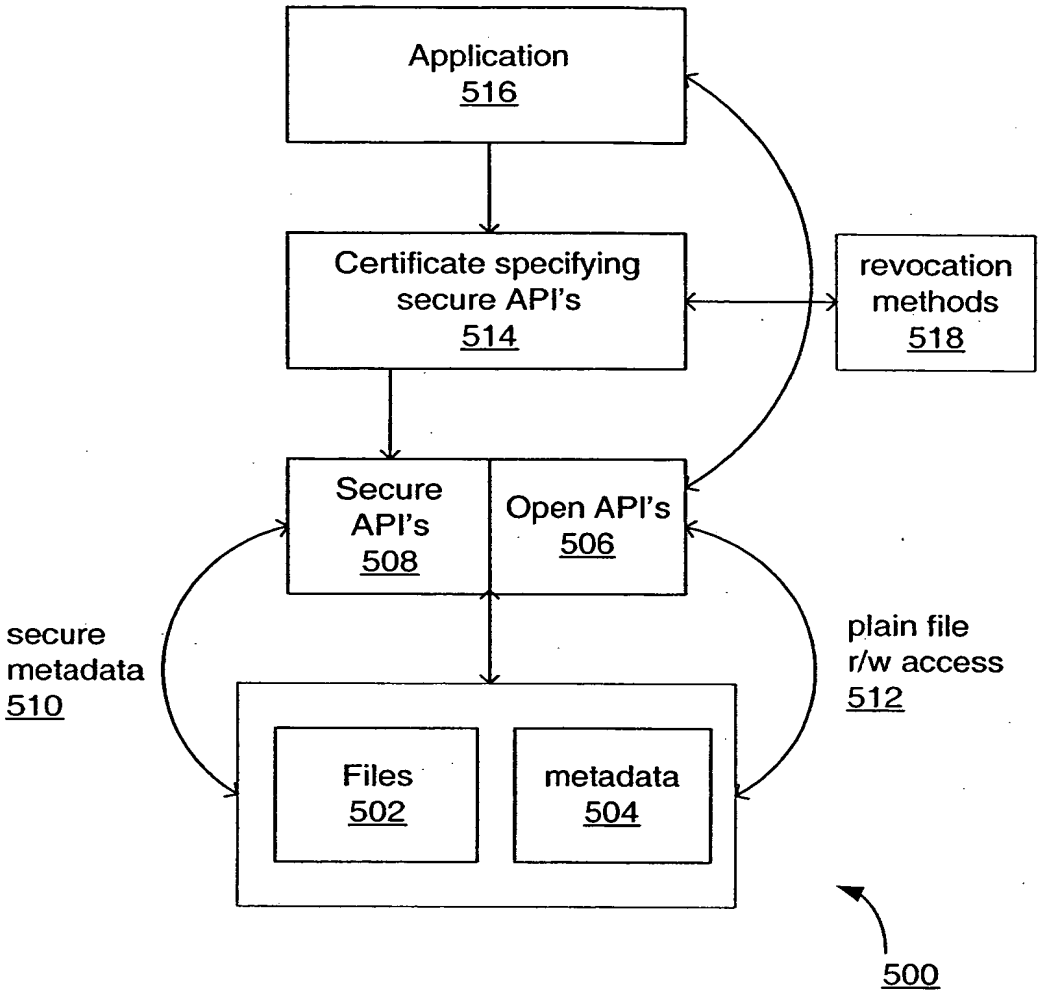


FIG. 5A

0540025 - 082701

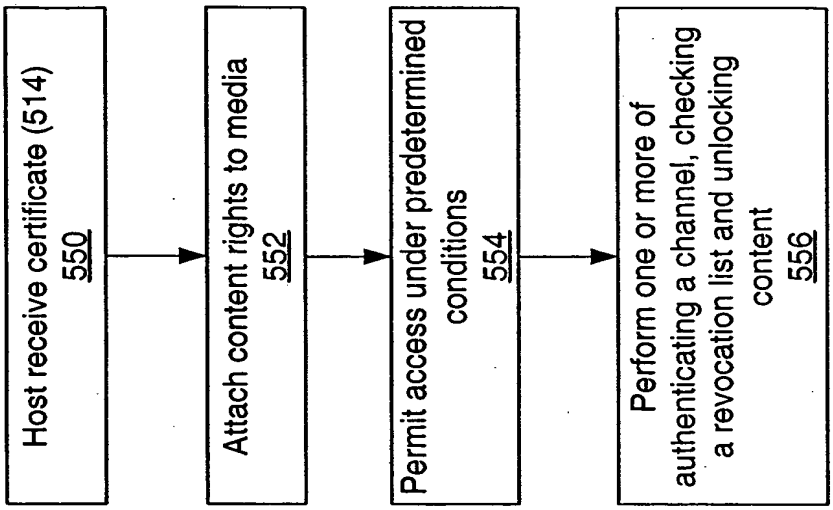


FIG. 5C

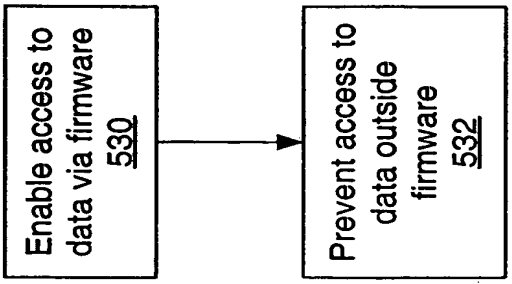


FIG. 5B

EL 728 "9 20 04 US

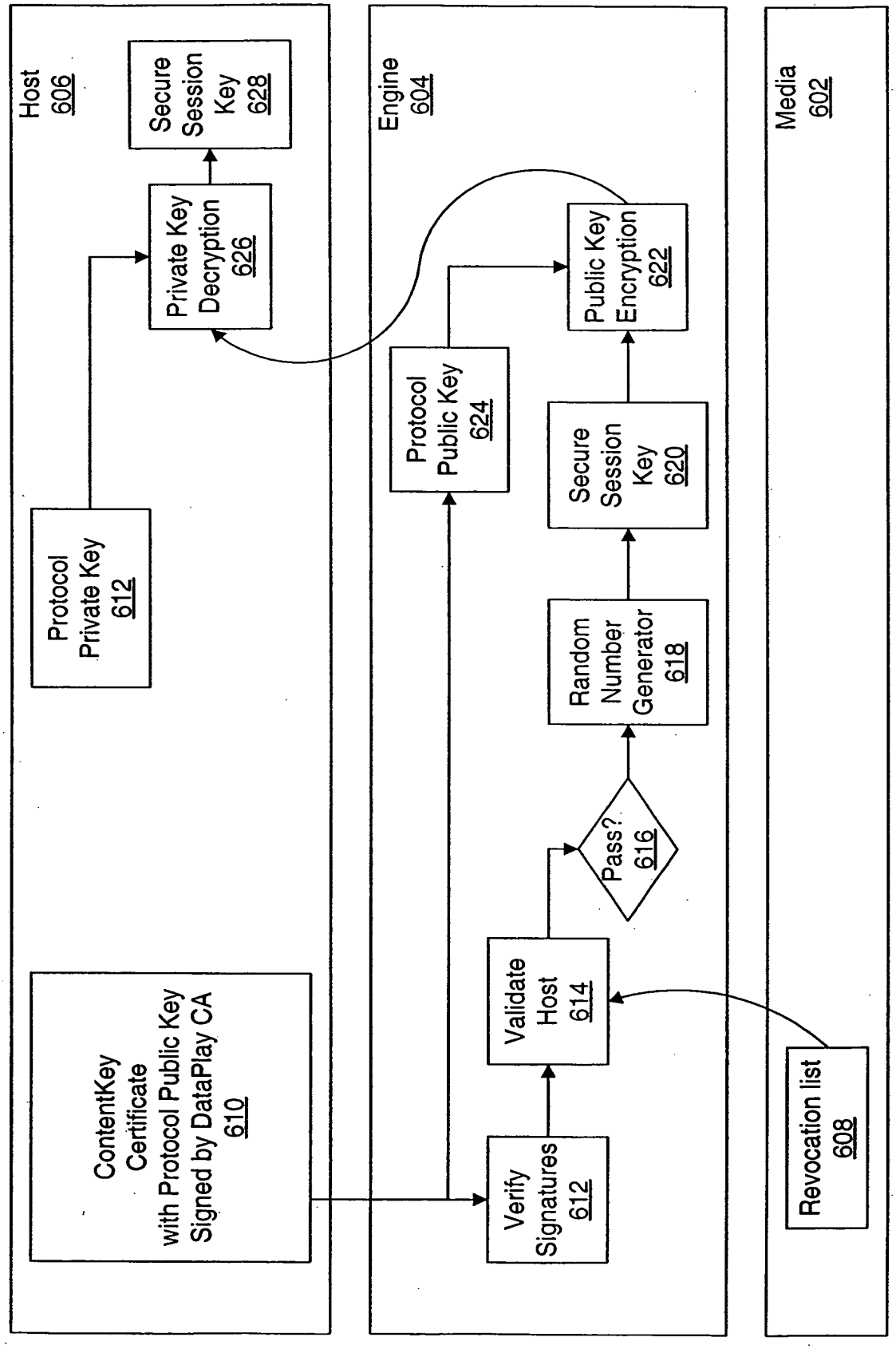

Host 606
Secure Session Key 628
Private Key Decryption 626
Protocol Private Key 612
ContentKey Certificate with Protocol Public Key Signed by DataPlay CA 610
Engine 604
Protocol Public Key 624
Public Key Encryption 622
Secure Session Key 620
Random Number Generator 618
Pass? 616
Validate Host 614
Verify Signatures 612
Media 602
Revocation list 608

FIG. 6

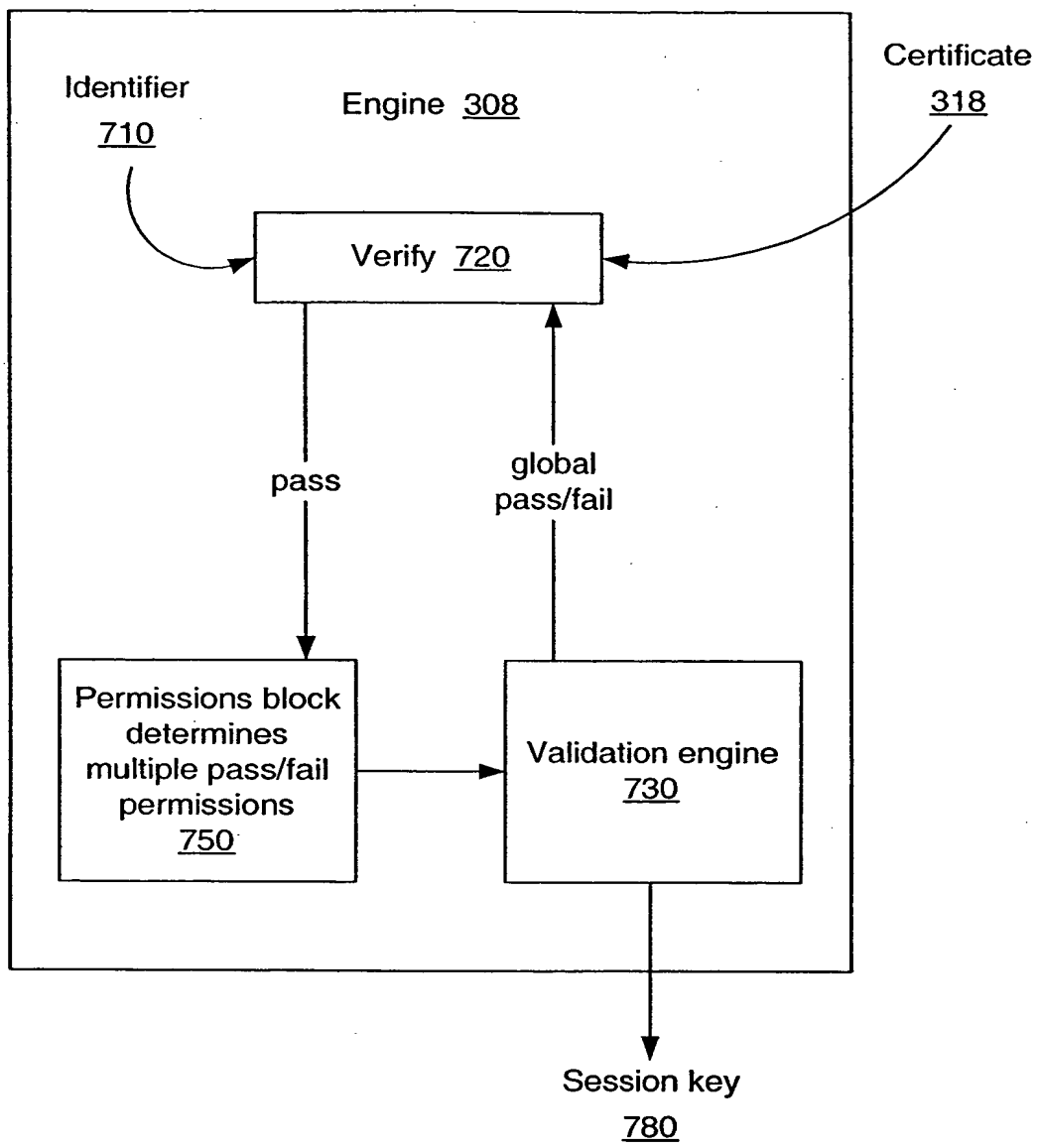


FIG. 7A

Docket #: 92026.0257.01

TO7280 9200h660

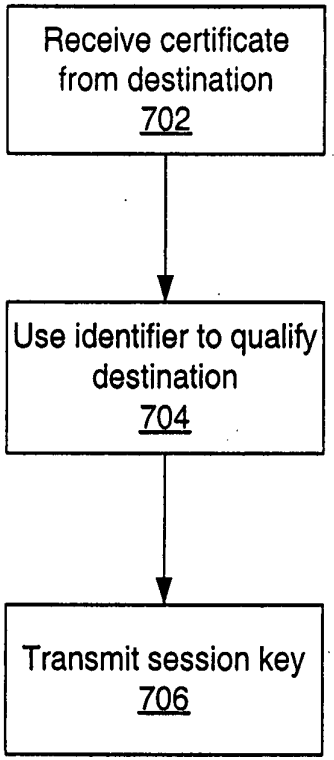


FIG. 7B

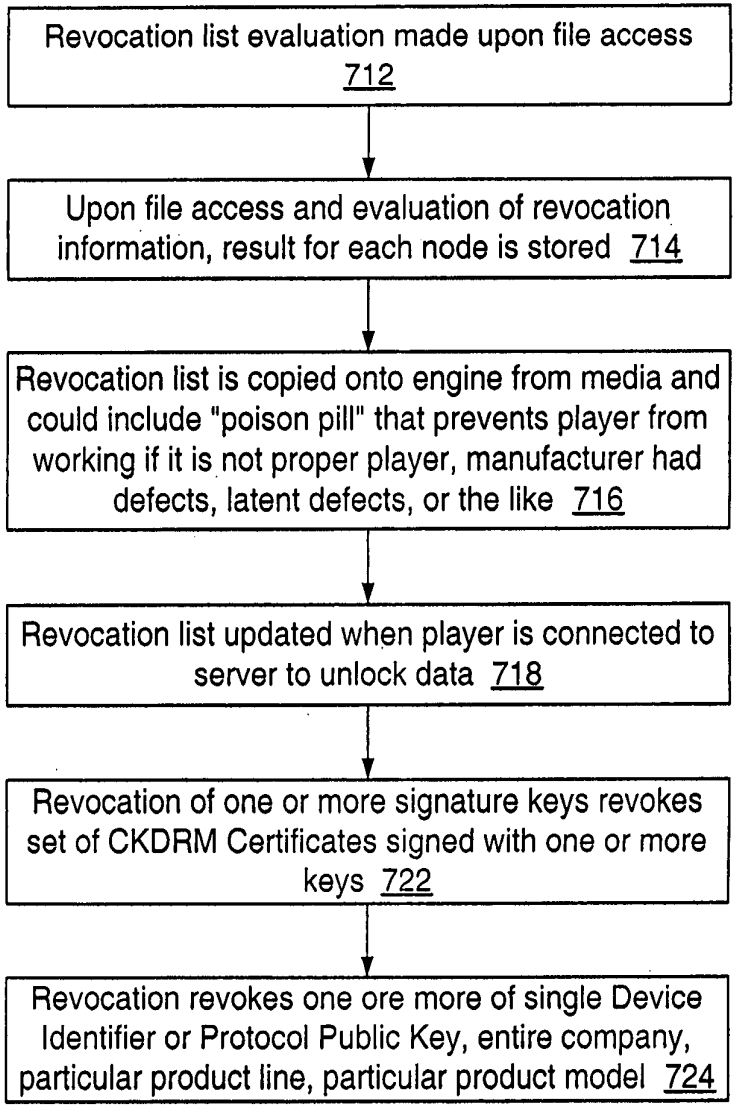


FIG. 7C

TO2280"9200H660

Attorney Docket No.: M-12041 US
First Inventor: Lane W. Lee
Title: Host Certification Method and System

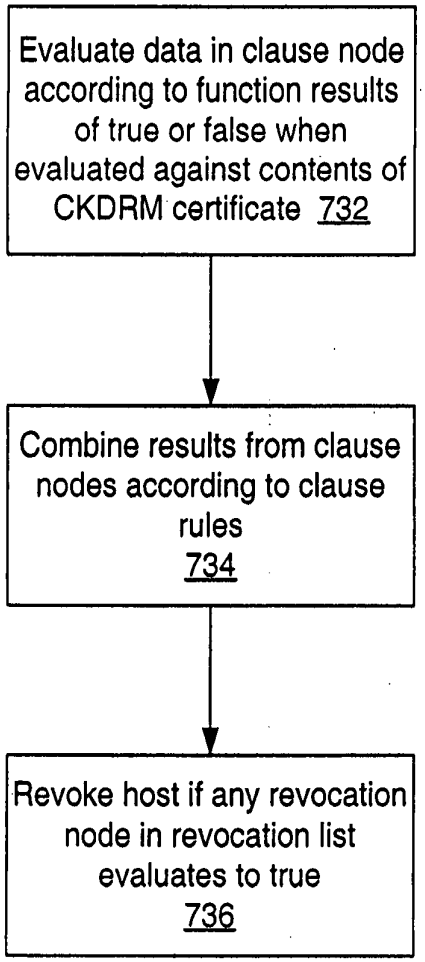


FIG. 7D

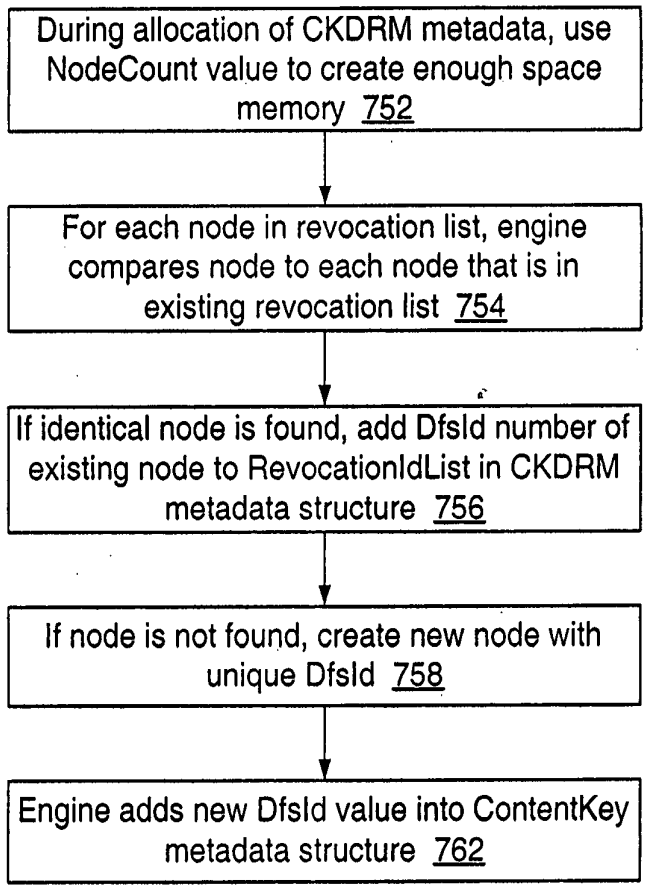


FIG. 7E

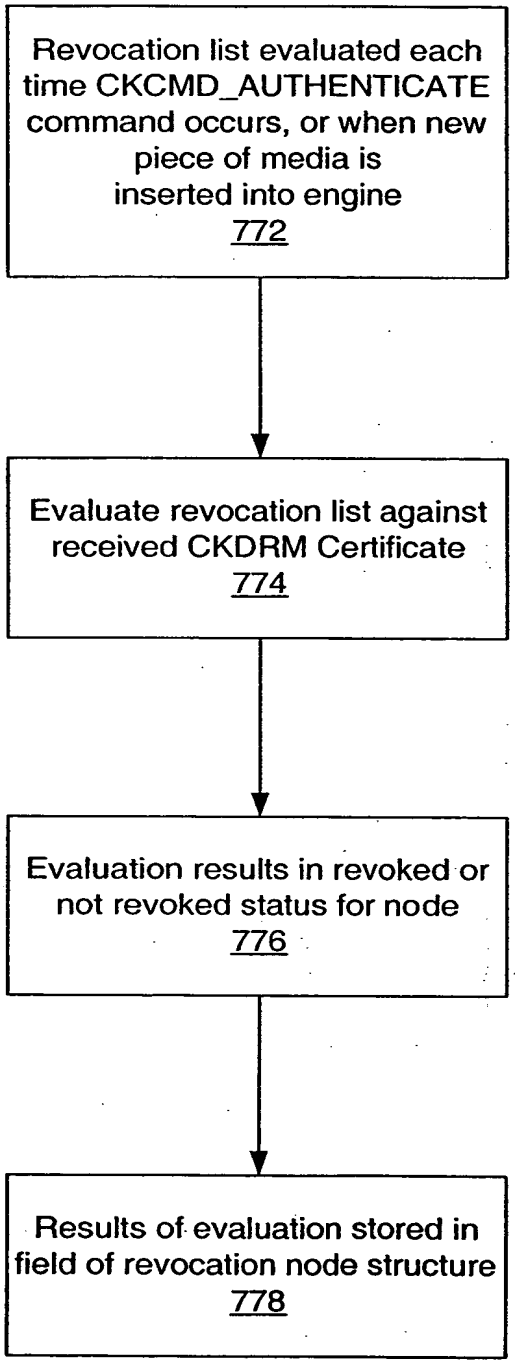


FIG. 7F

09540026-082504

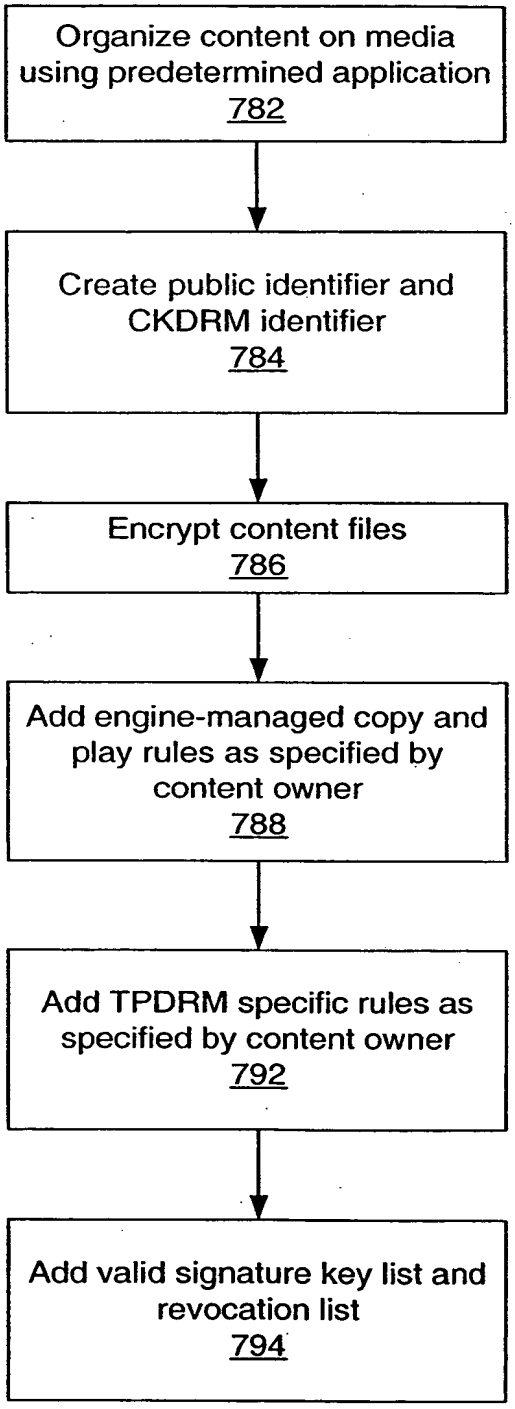


FIG. 7G

9540825.082701

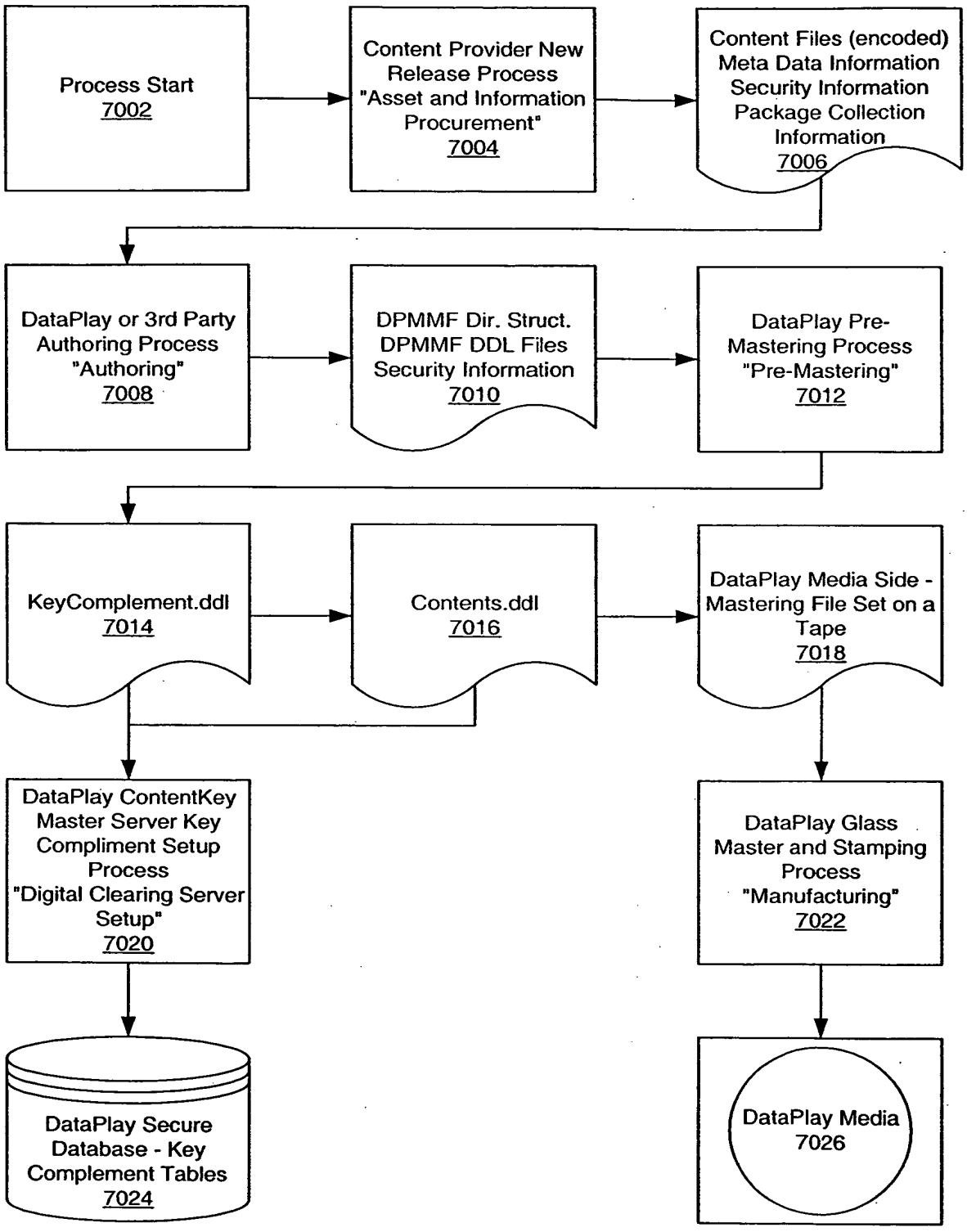


FIG. 7H

Docket #M-12041 US

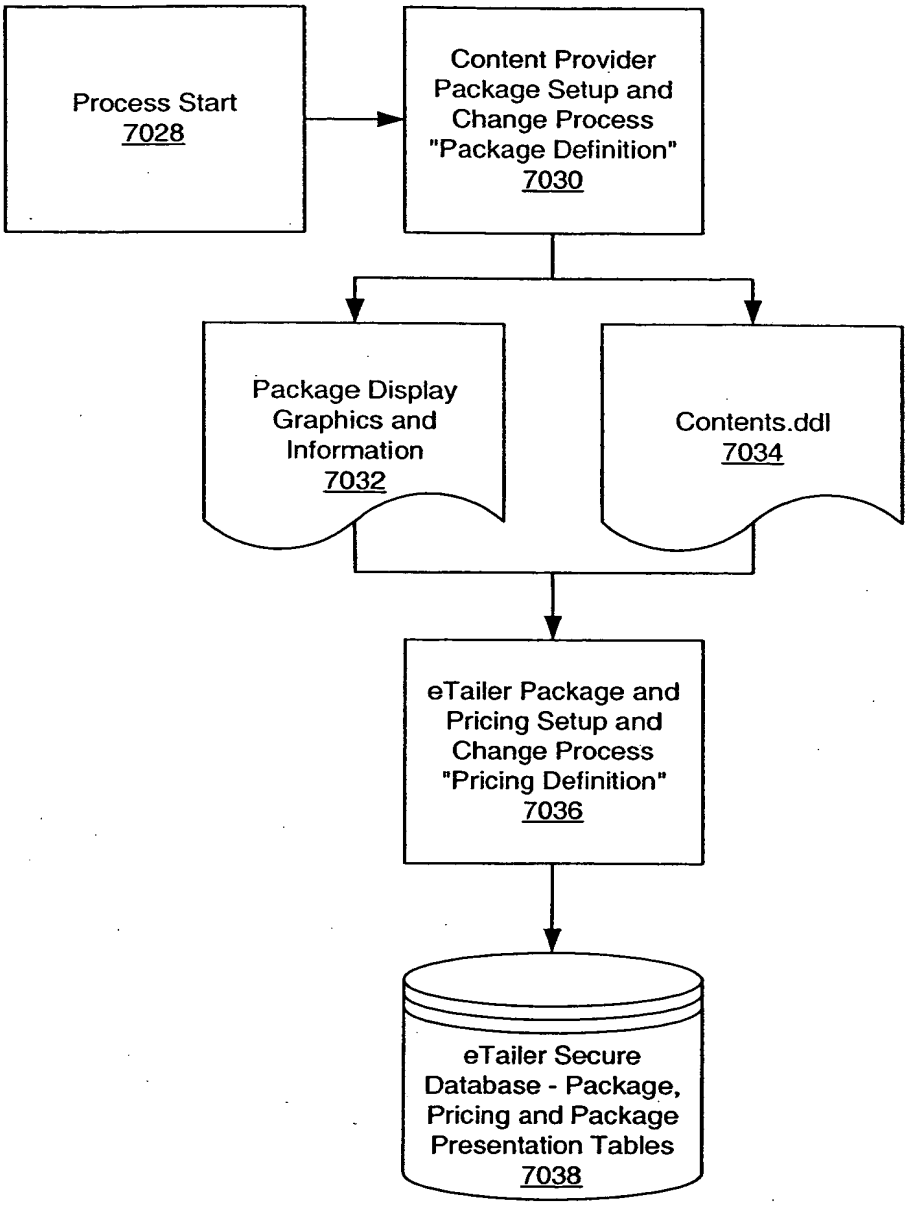


FIG. 7I

09540026 - 082701

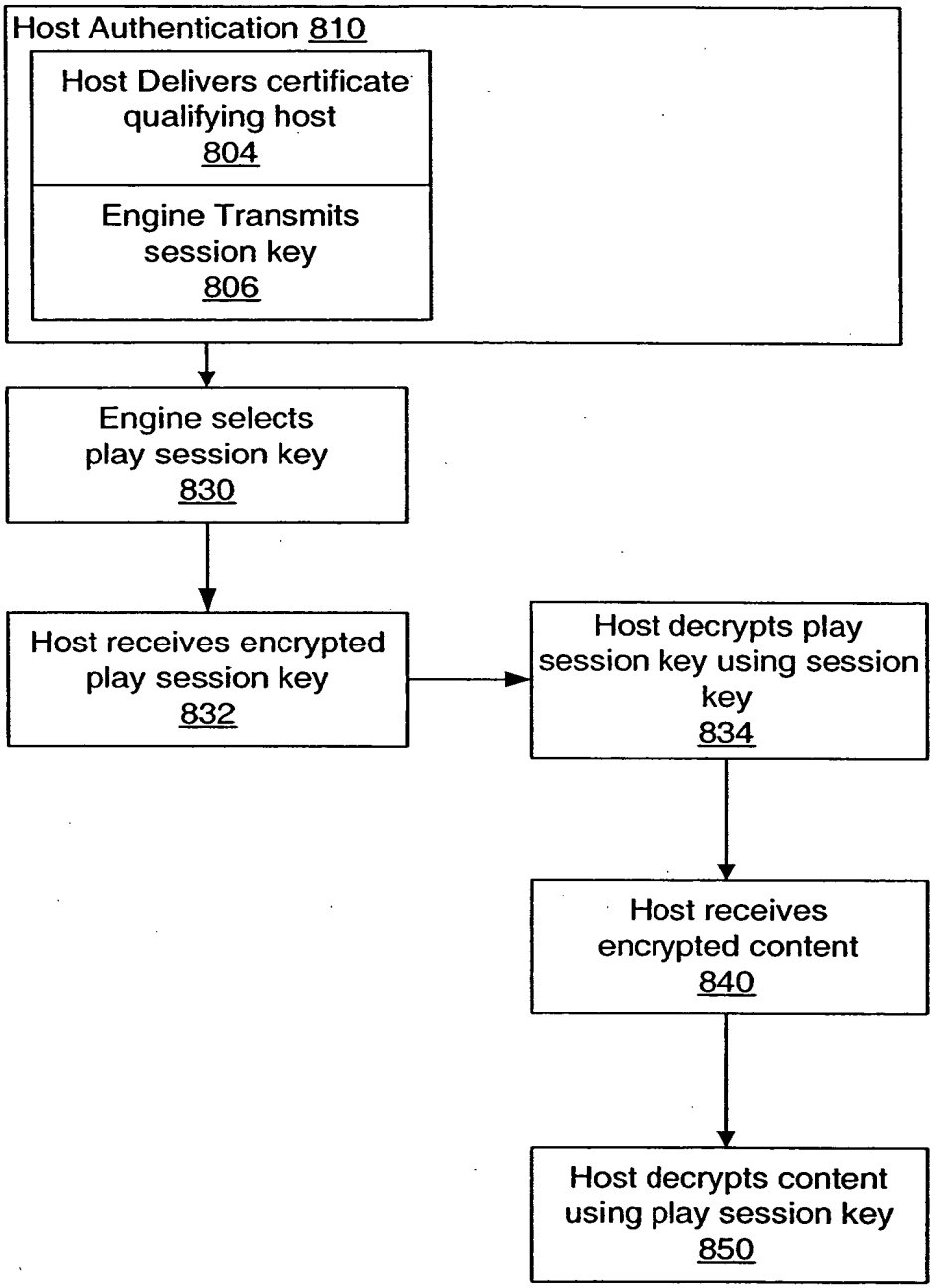


FIG. 8

09400626 - 082701

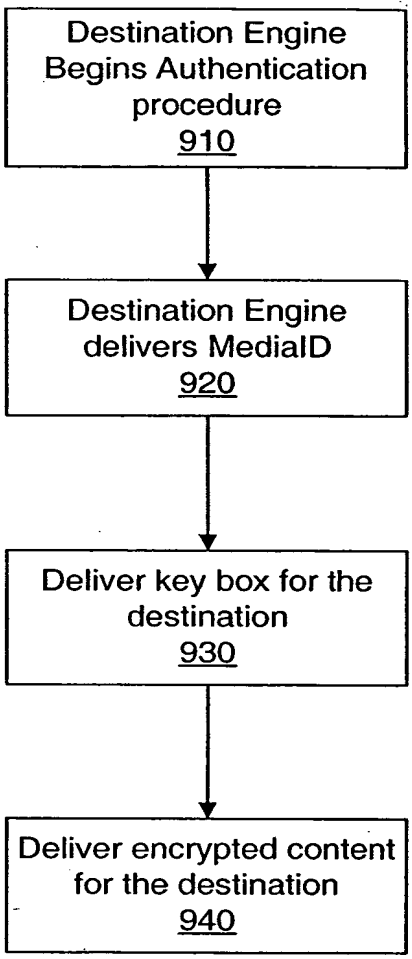


FIG. 9

09540026 - 082701

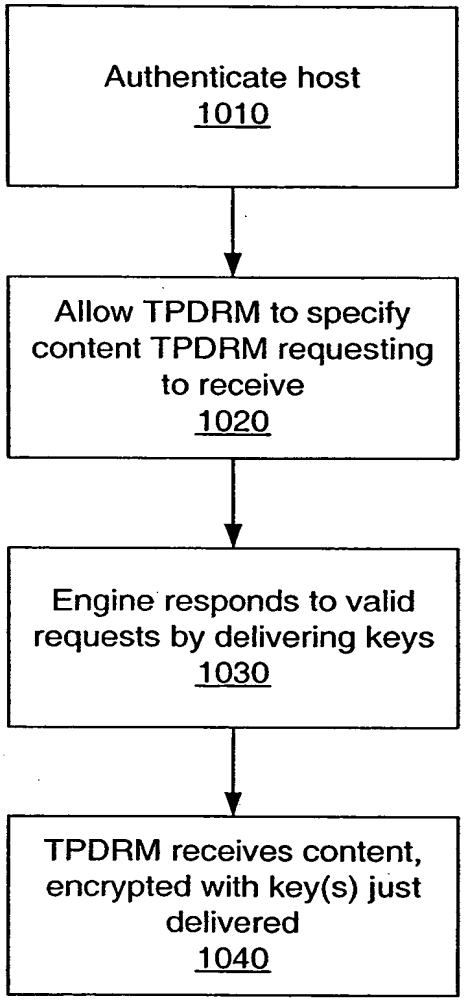


FIG. 10

EXPRESS MAIL NO. EV 340026 US

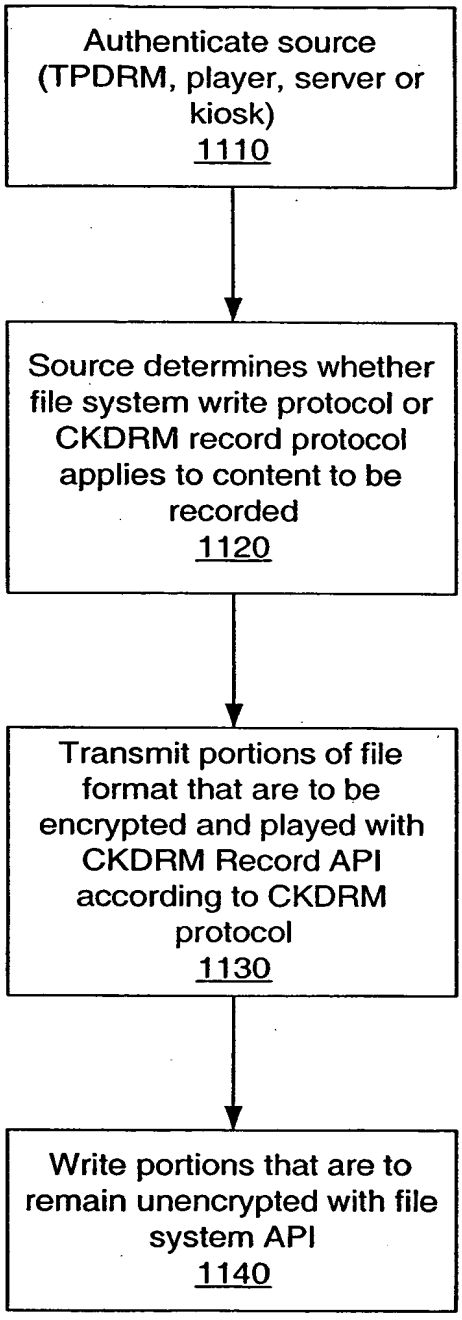


FIG. 11

Express Mail Label No. EV 340025970 US

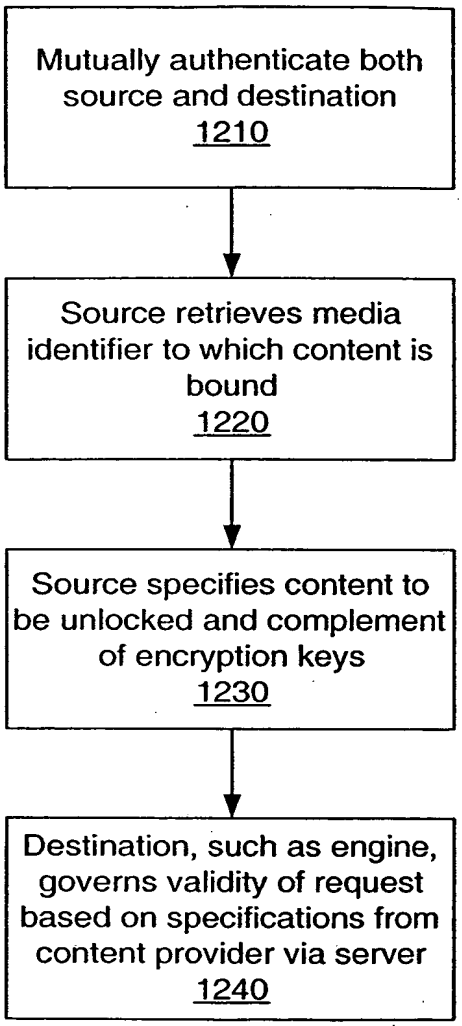


FIG. 12

Express Mail Label No. EV 720 926 504 US

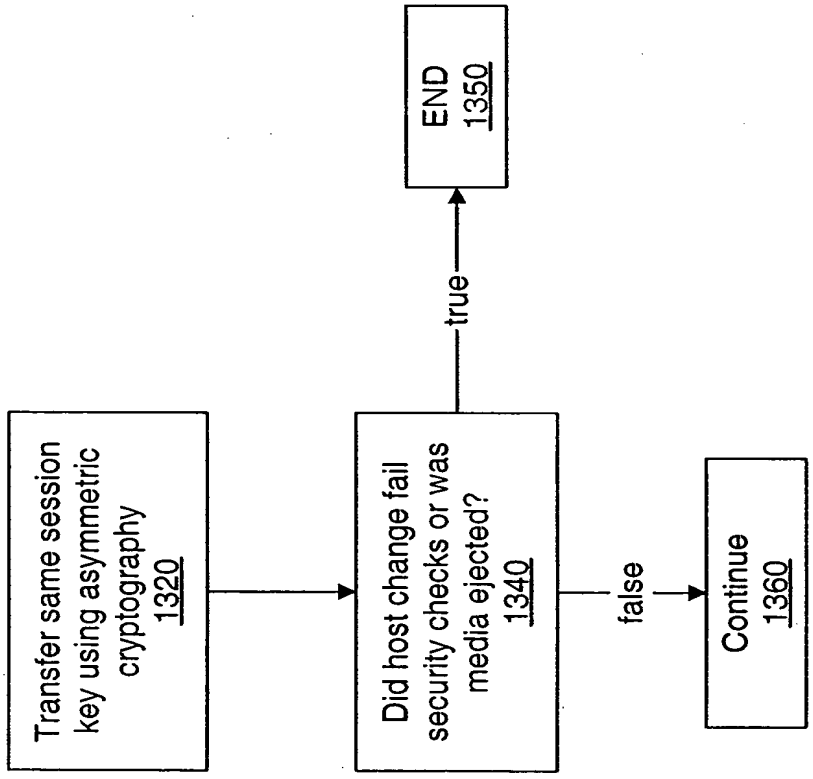

Transfer same session key using asymmetric cryptography 1320
Did host change fail security checks or was media ejected? 1340
true
END 1350
false
Continue 1360

FIG. 13

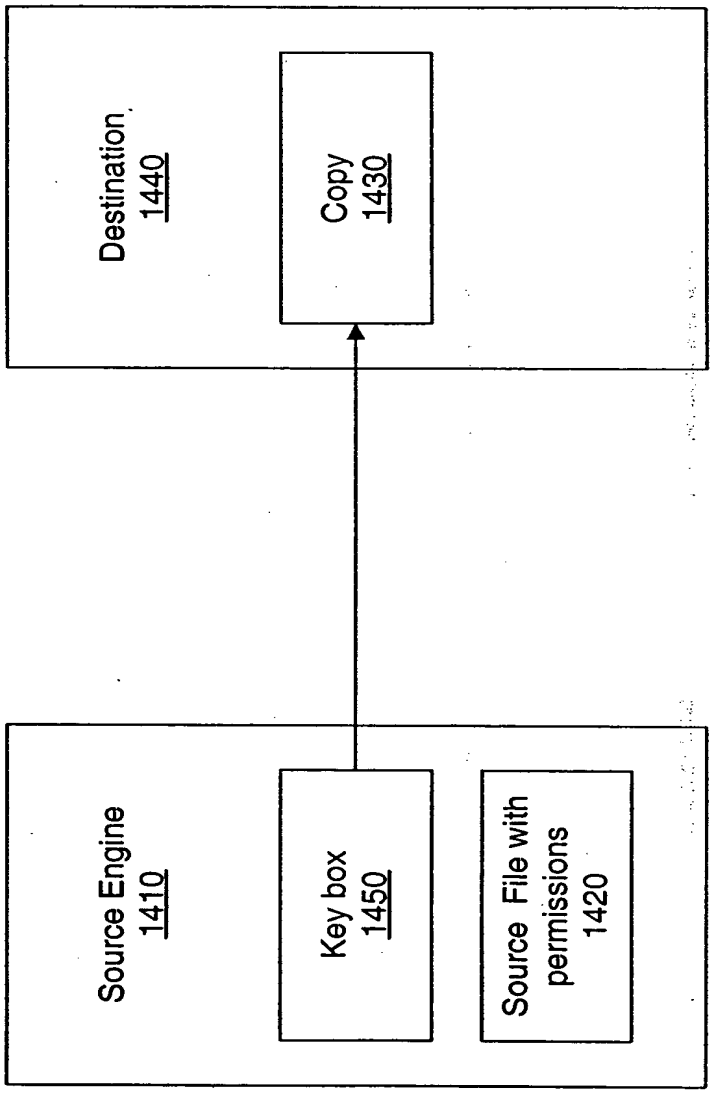


FIG. 14

T-072 P.080/080 F-920

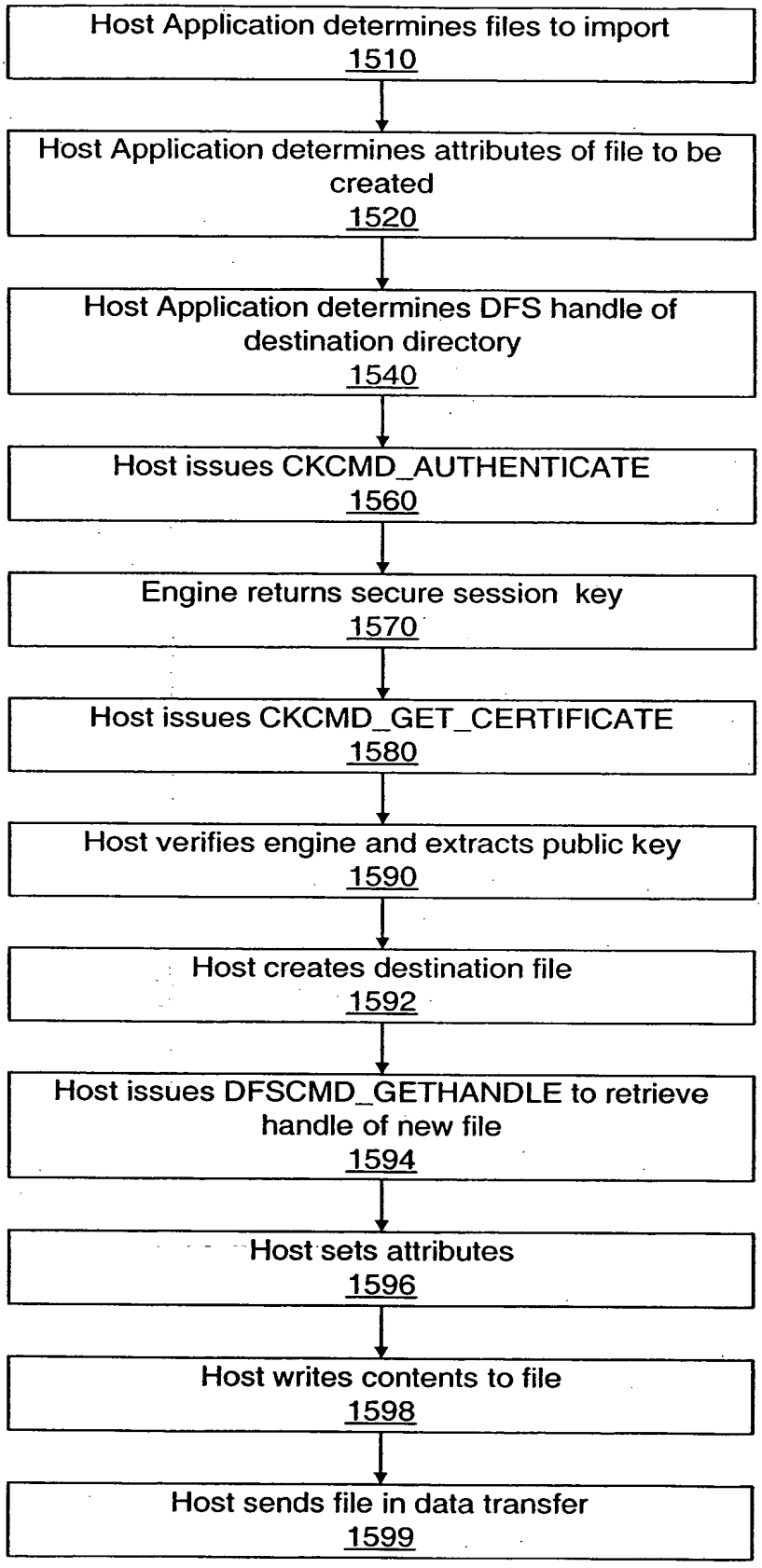


FIG. 15

TO/2005-0802-0960-01

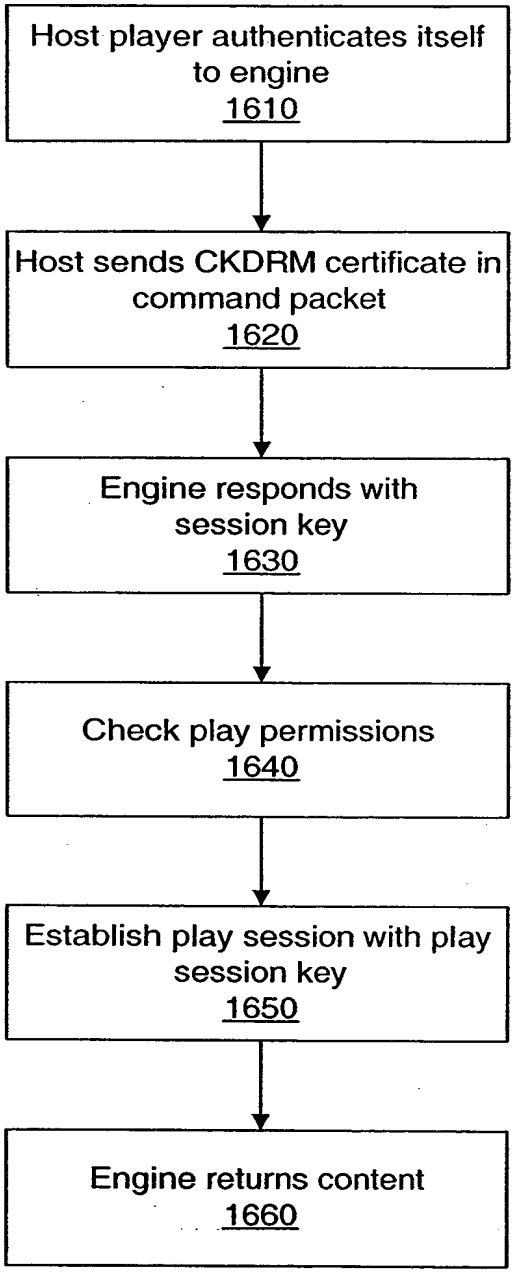


FIG. 16

Express Mail No. EV 329 805 025 US

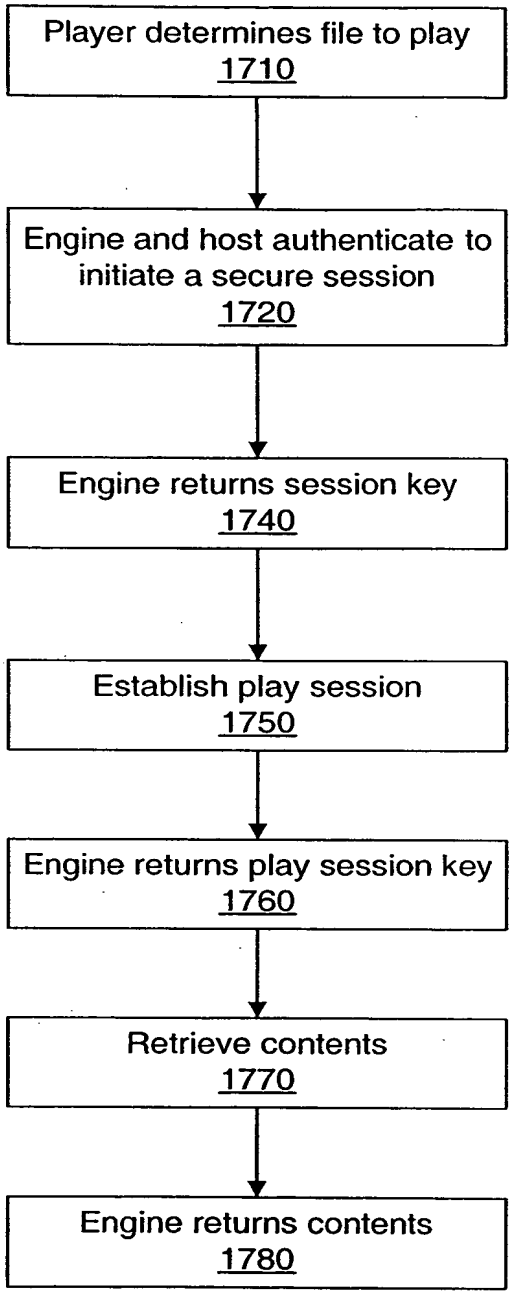


FIG. 17

Express Mail Label No. EV 760 026 945 US

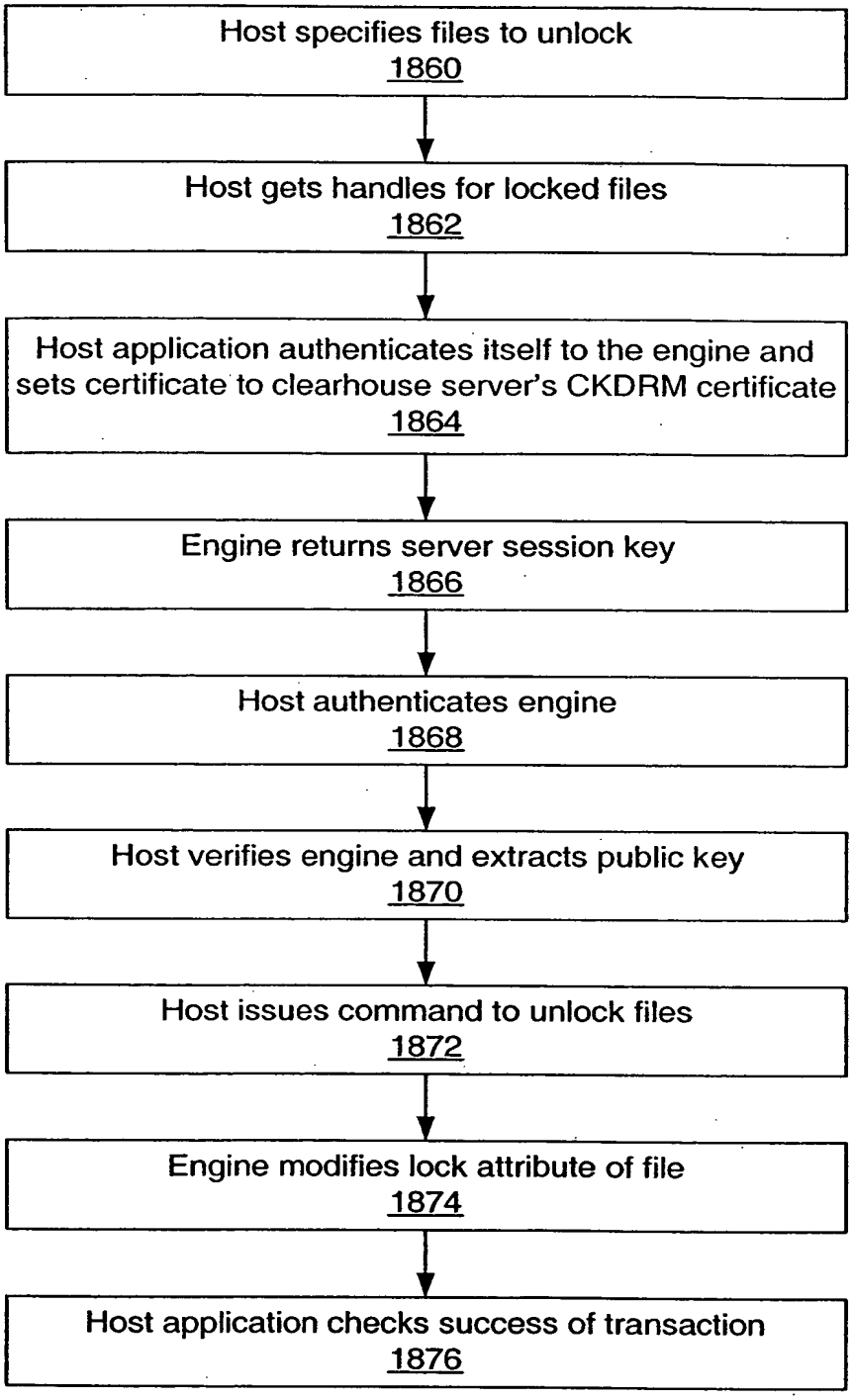


FIG. 18

Client-Ex. 1026 - 0394026

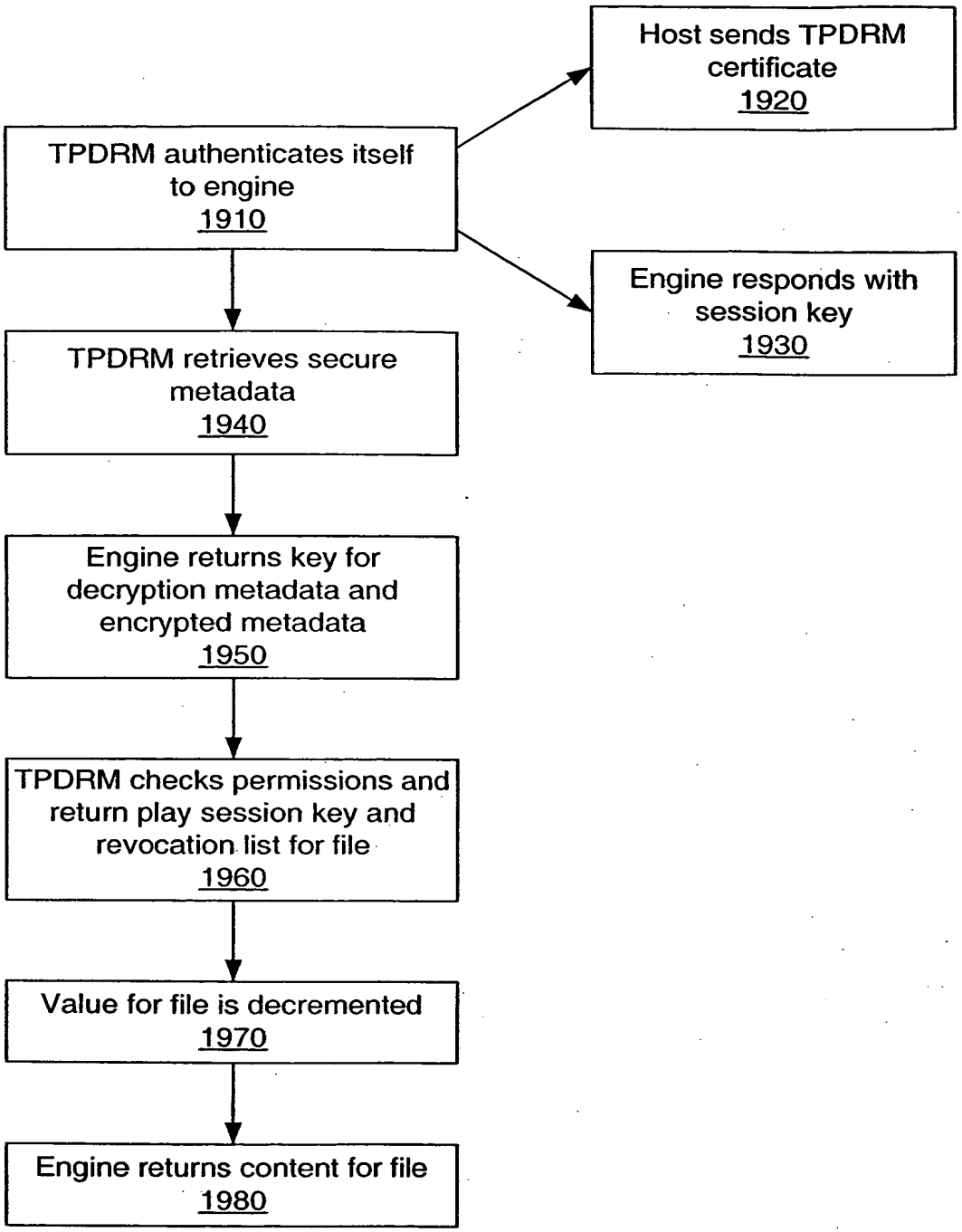

TPDRM authenticates itself to engine
1910
Host sends TPDRM certificate
1920
Engine responds with session key
1930
TPDRM retrieves secure metadata
1940
Engine returns key for decryption metadata and encrypted metadata
1950
TPDRM checks permissions and return play session key and revocation list for file
1960
Value for file is decremented
1970
Engine returns content for file
1980

FIG. 19

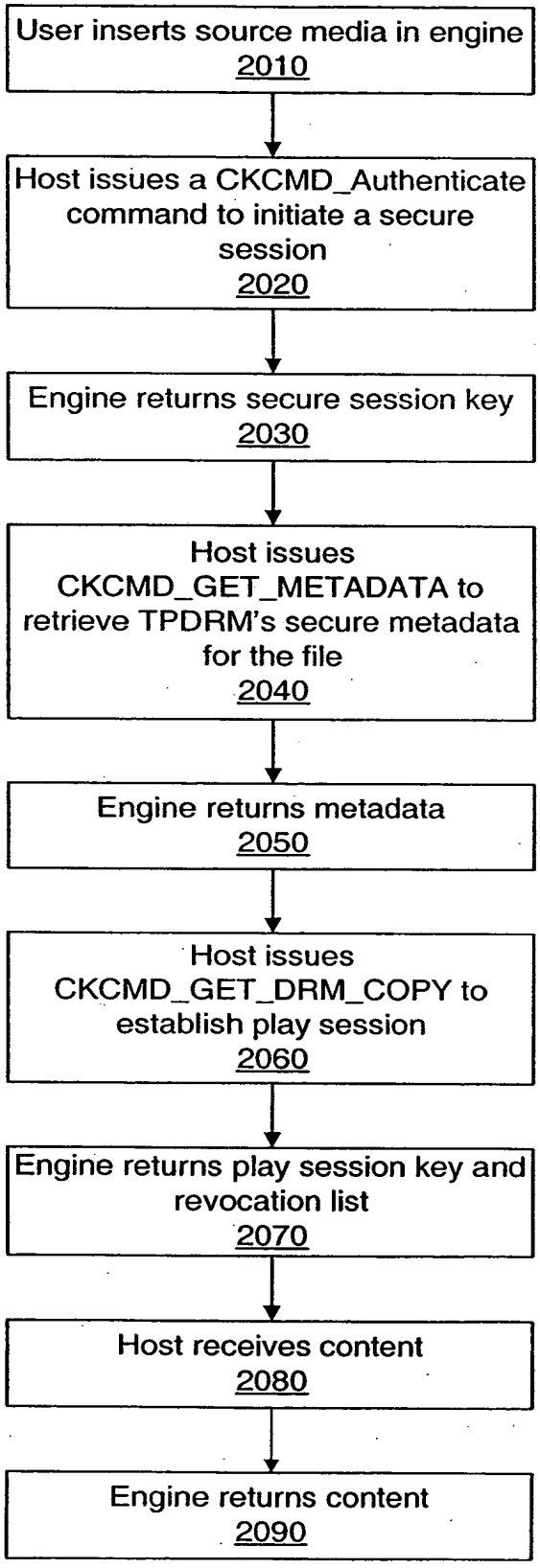


FIG. 20

EV 280 250 704 US

Express Mail Label No. EV 278026845 US

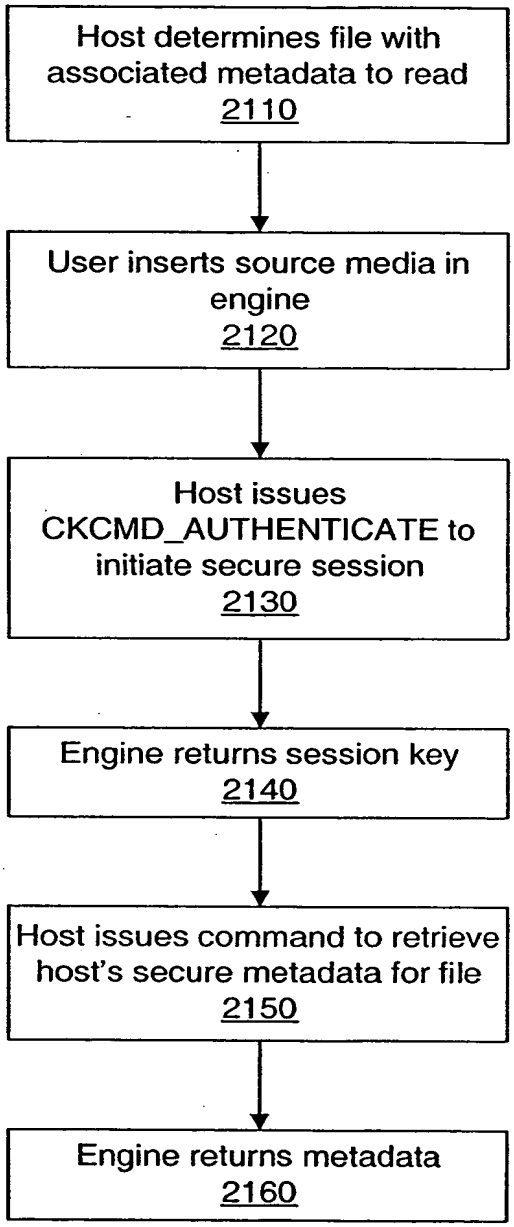


FIG. 21

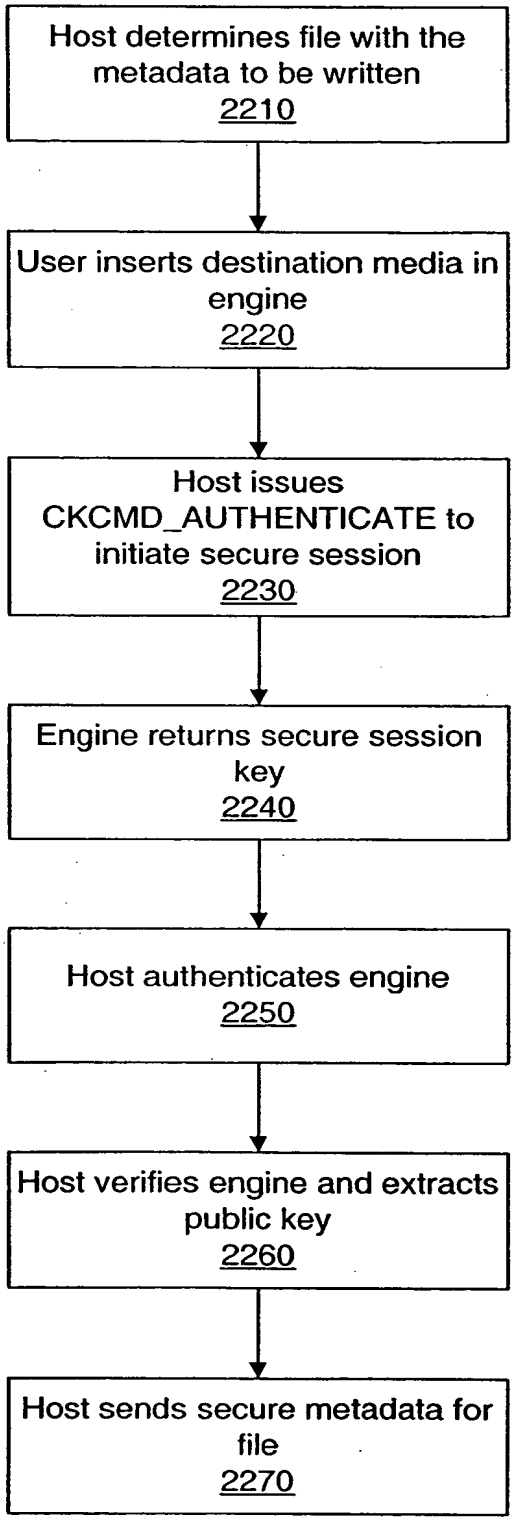


FIG. 22A

Express Mail Label No. EV329080460

PD-203204.6.0

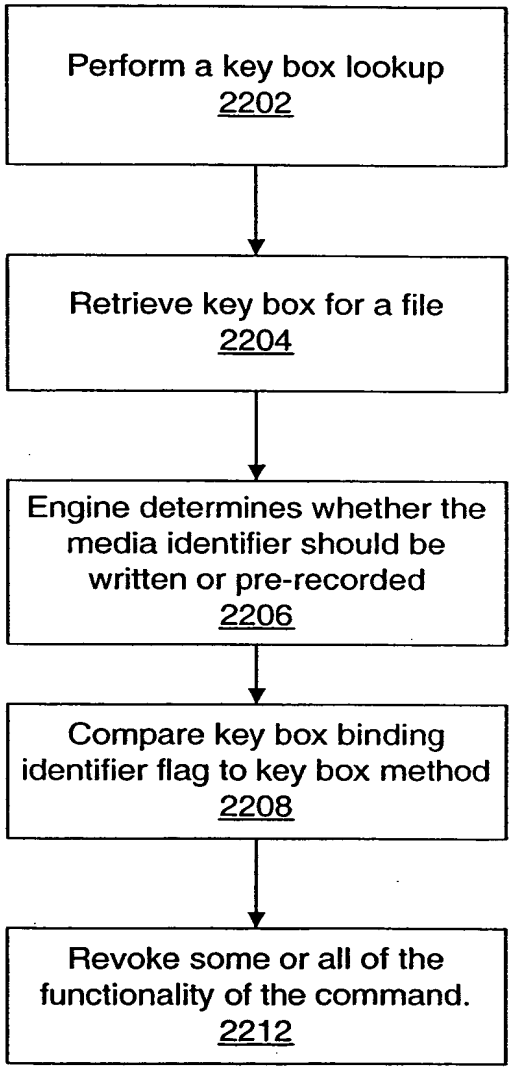


FIG. 22B

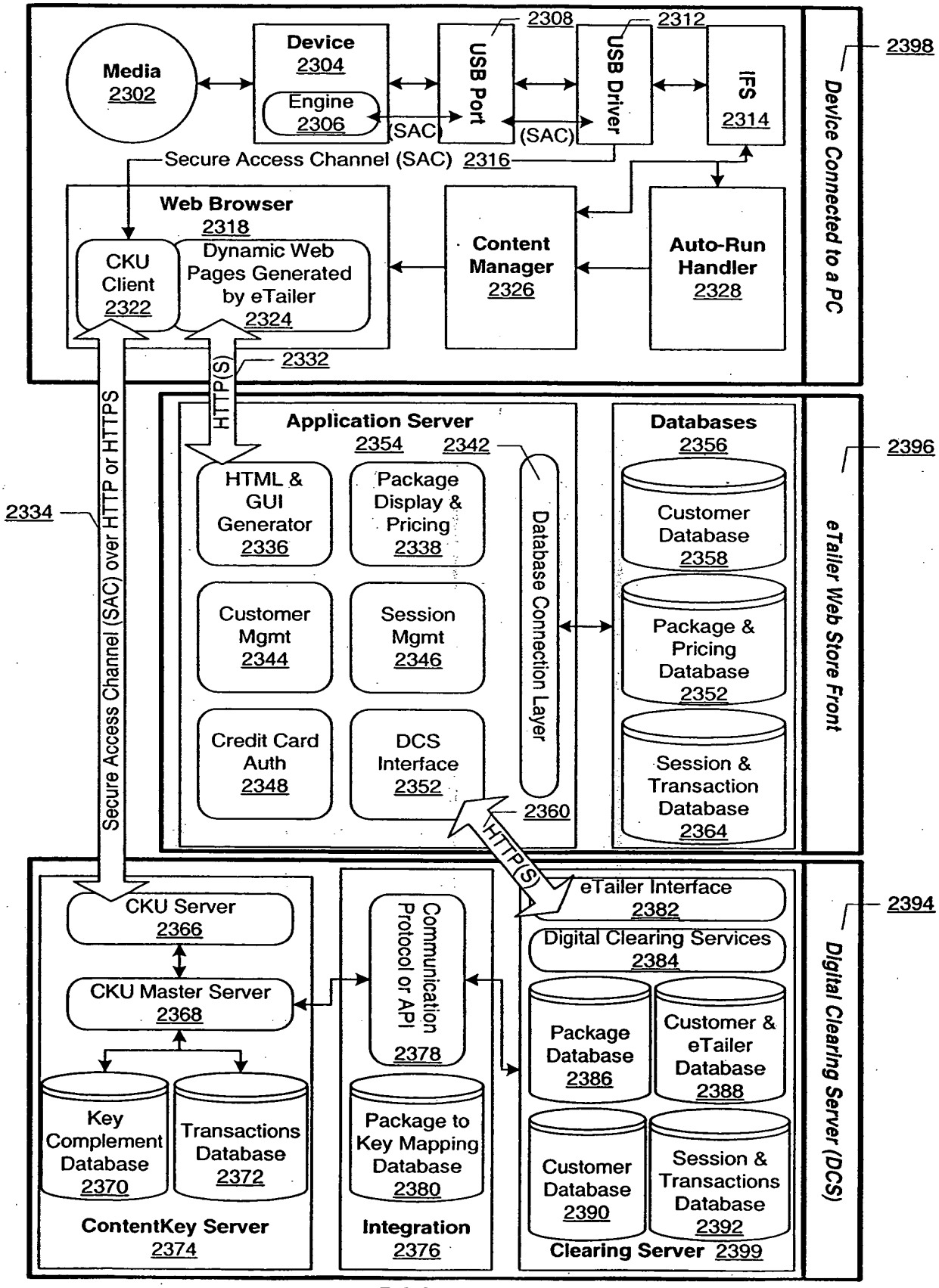


FIG. 23A

09400625 - 082701

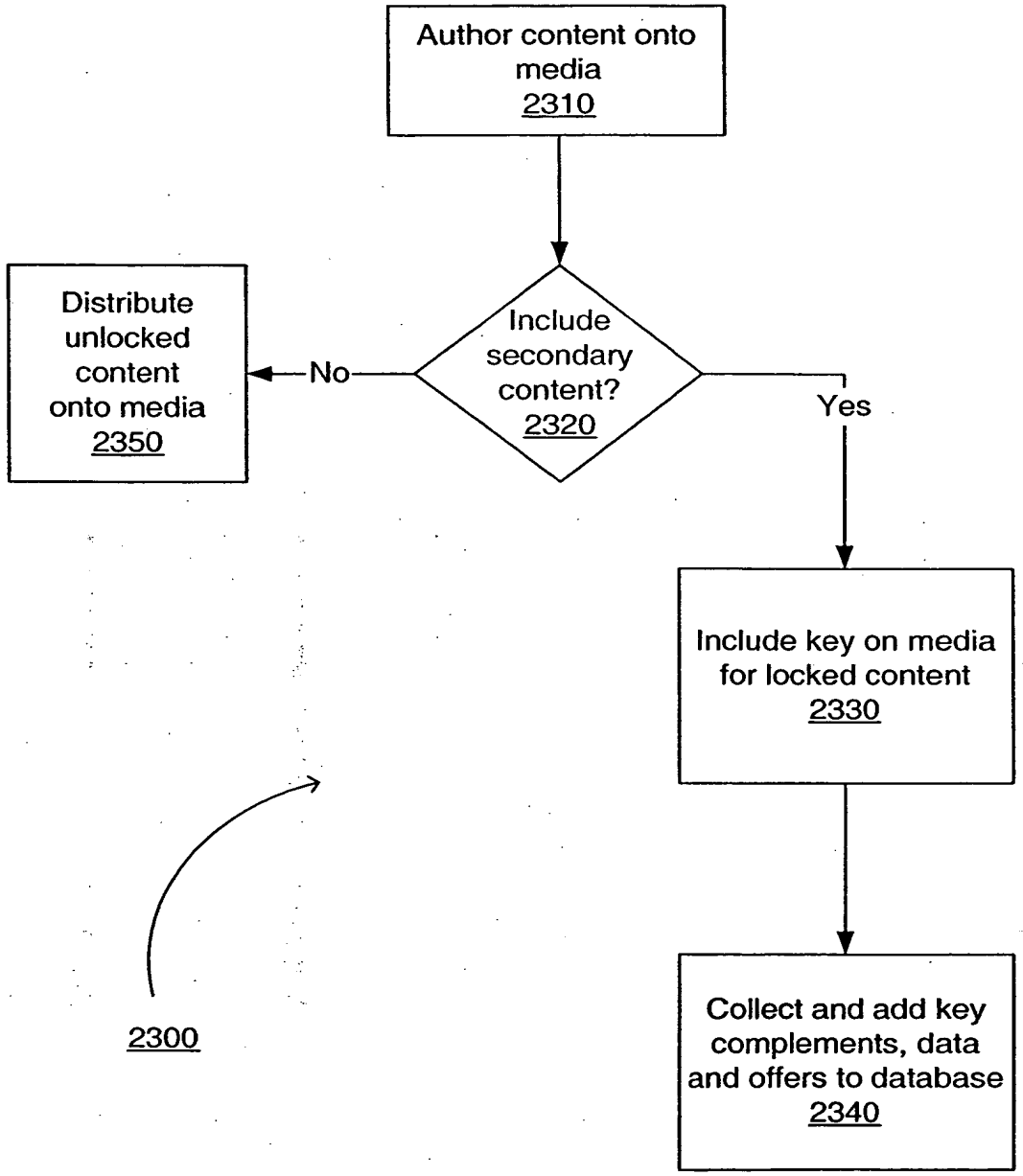

Author content onto media 2310
Include secondary content? 2320
No
Distribute unlocked content onto media 2350
Yes
Include key on media for locked content 2330
Collect and add key complements, data and offers to database 2340
2300

FIG. 23B

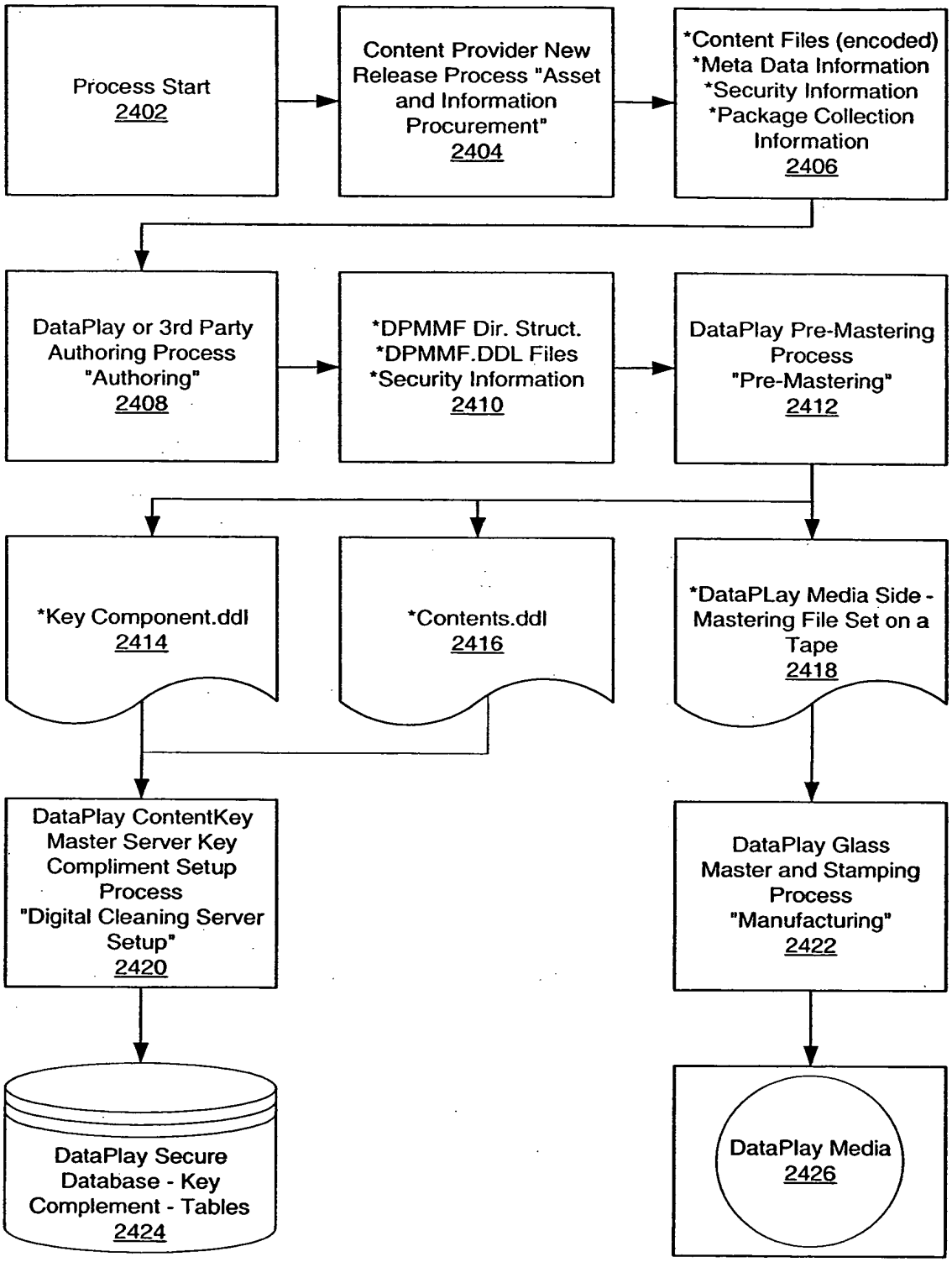


FIG. 24

09508025.082501

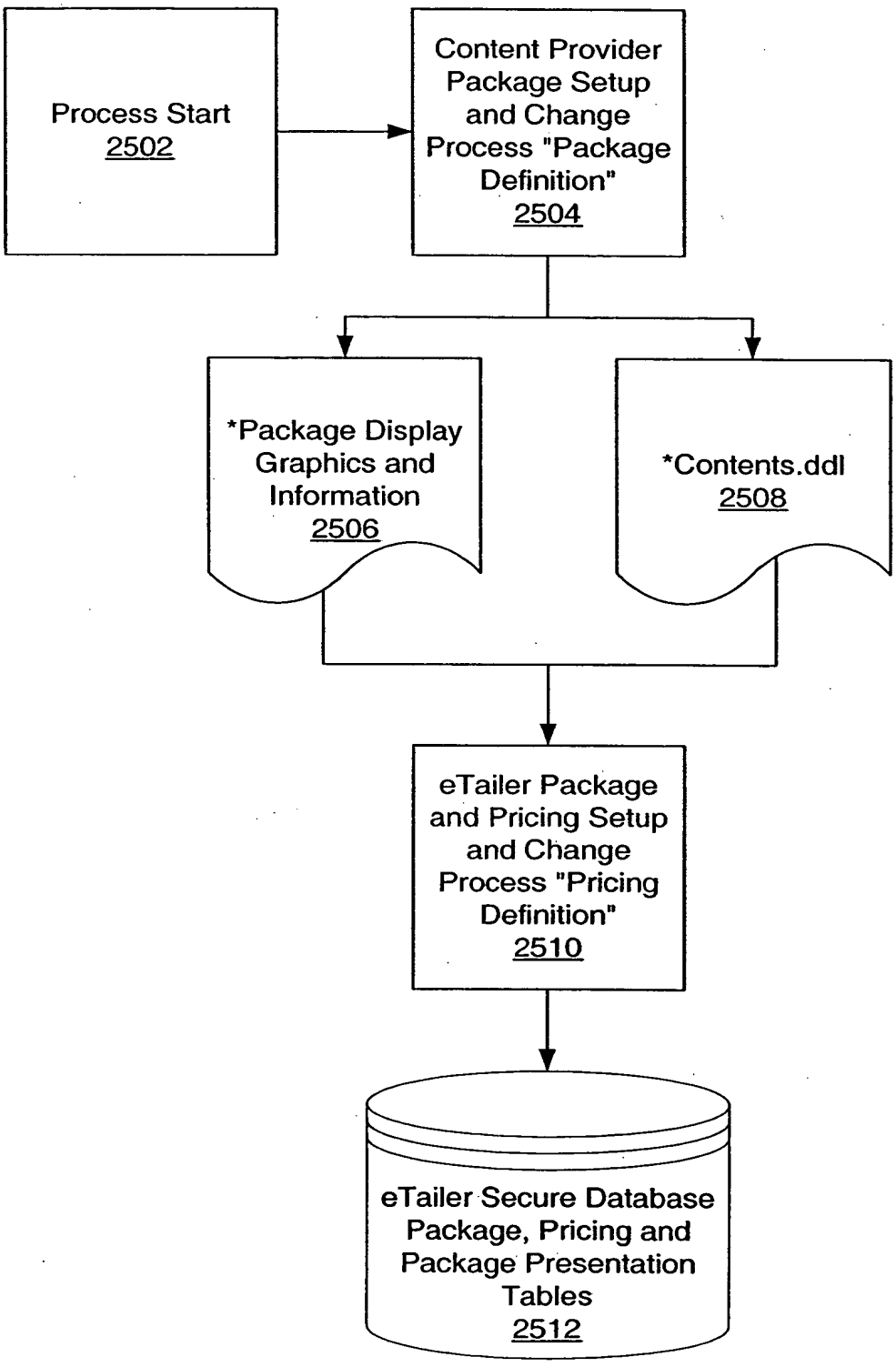


FIG. 25

09406026-062704

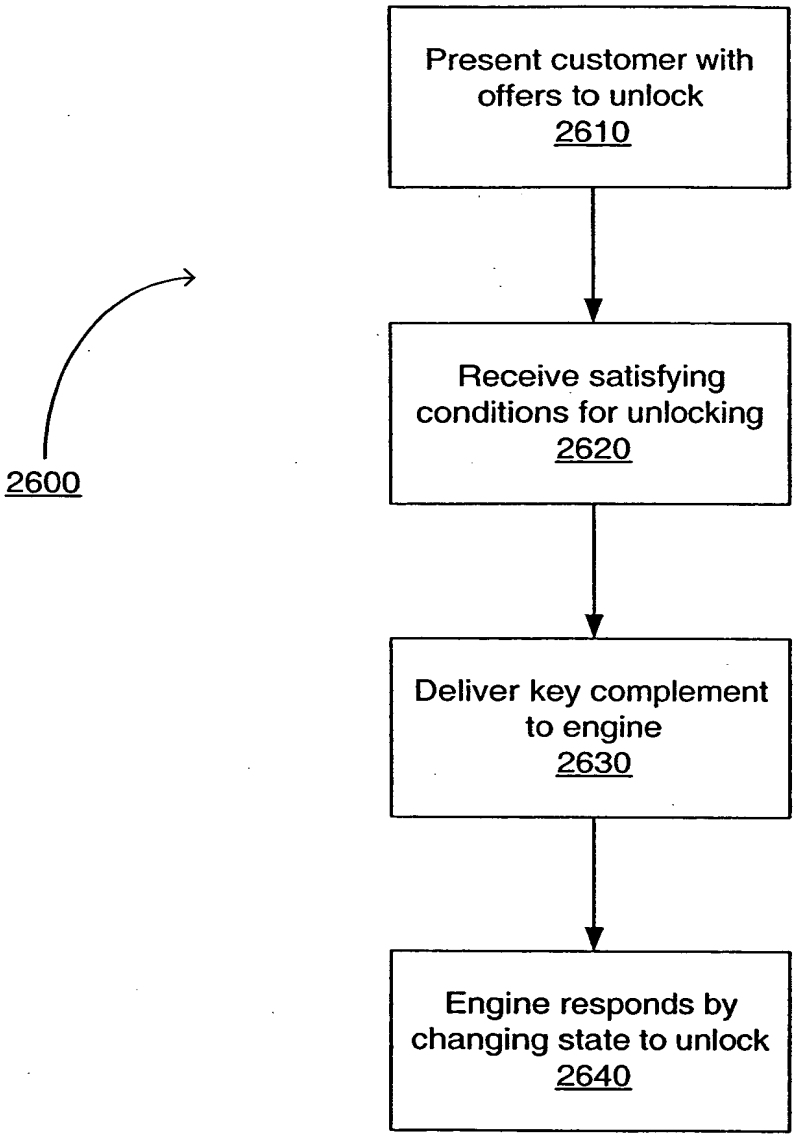
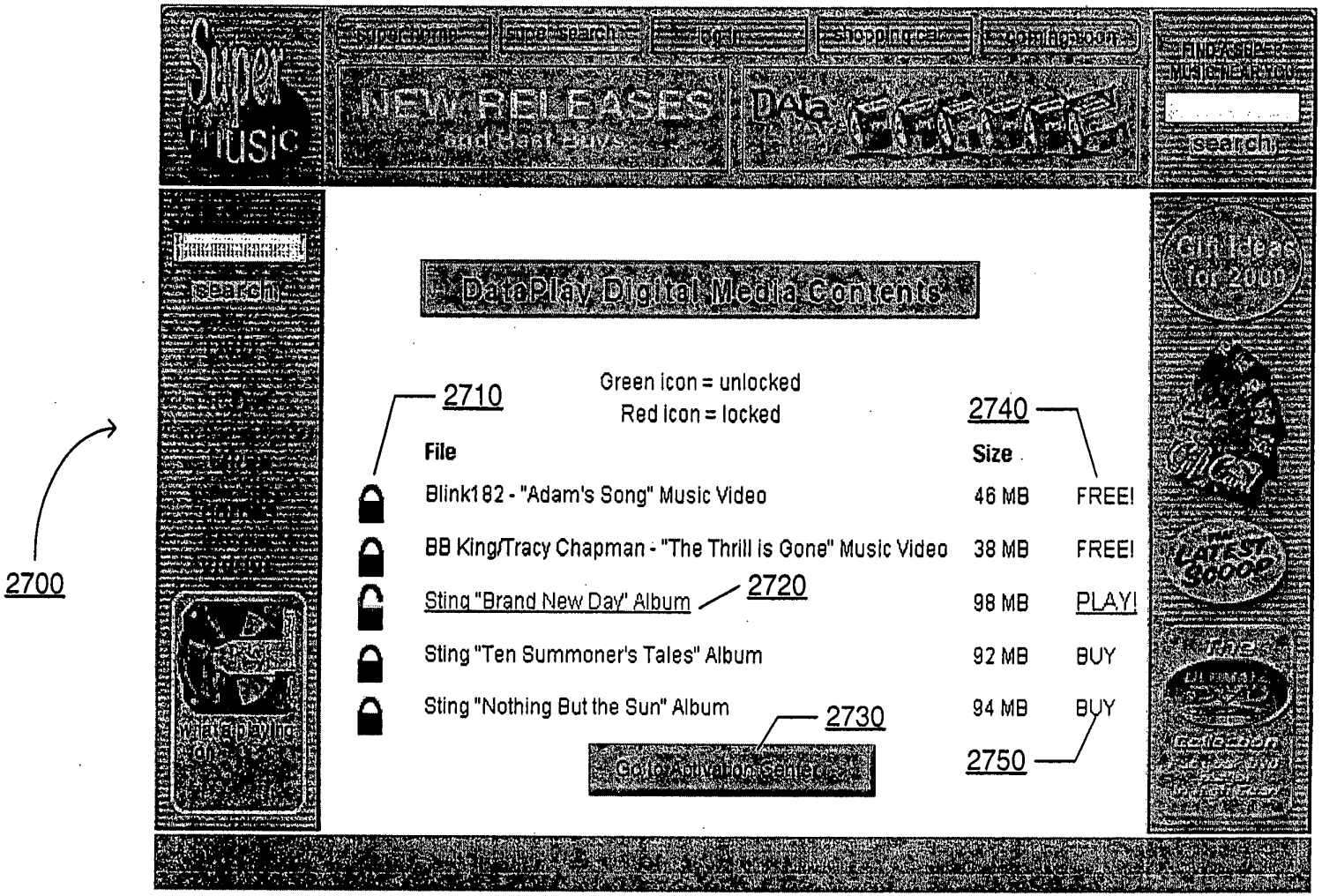


FIG. 26

05400326.082704

Attorney Docket No.: M-12041 US
First Inventor: Lane W. Lee
Title: Host Certification Method and System



2700

FIG. 27

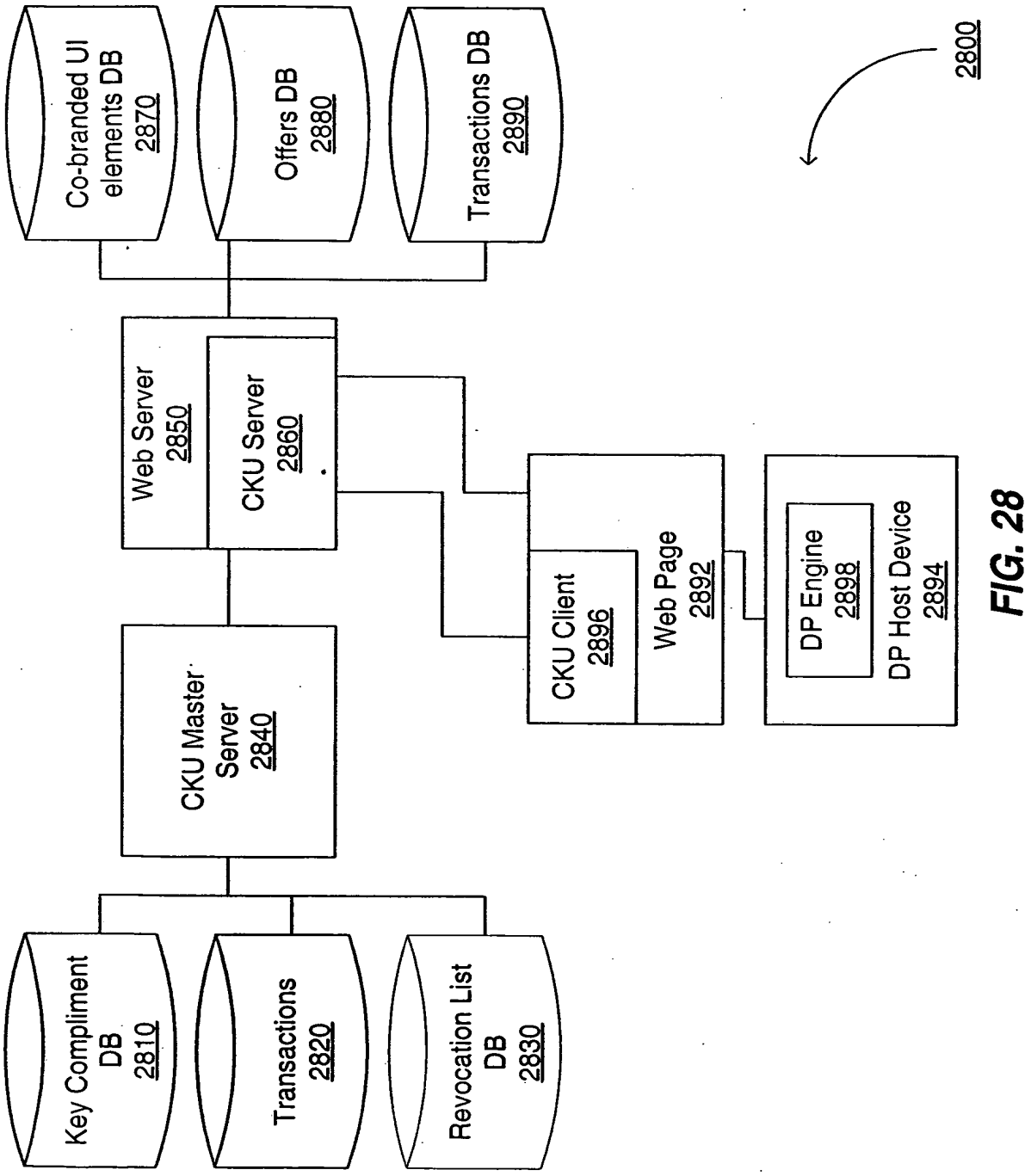

2800
Co-branded UI elements DB 2870
Offers DB 2880
Transactions DB 2890
Web Server 2850
CKU Server 2860
CKU Master Server 2840
CKU Client 2896
Web Page 2892
DP Engine 2898
DP Host Device 2894
Key Compliment DB 2810
Transactions 2820
Revocation List DB 2830

FIG. 28

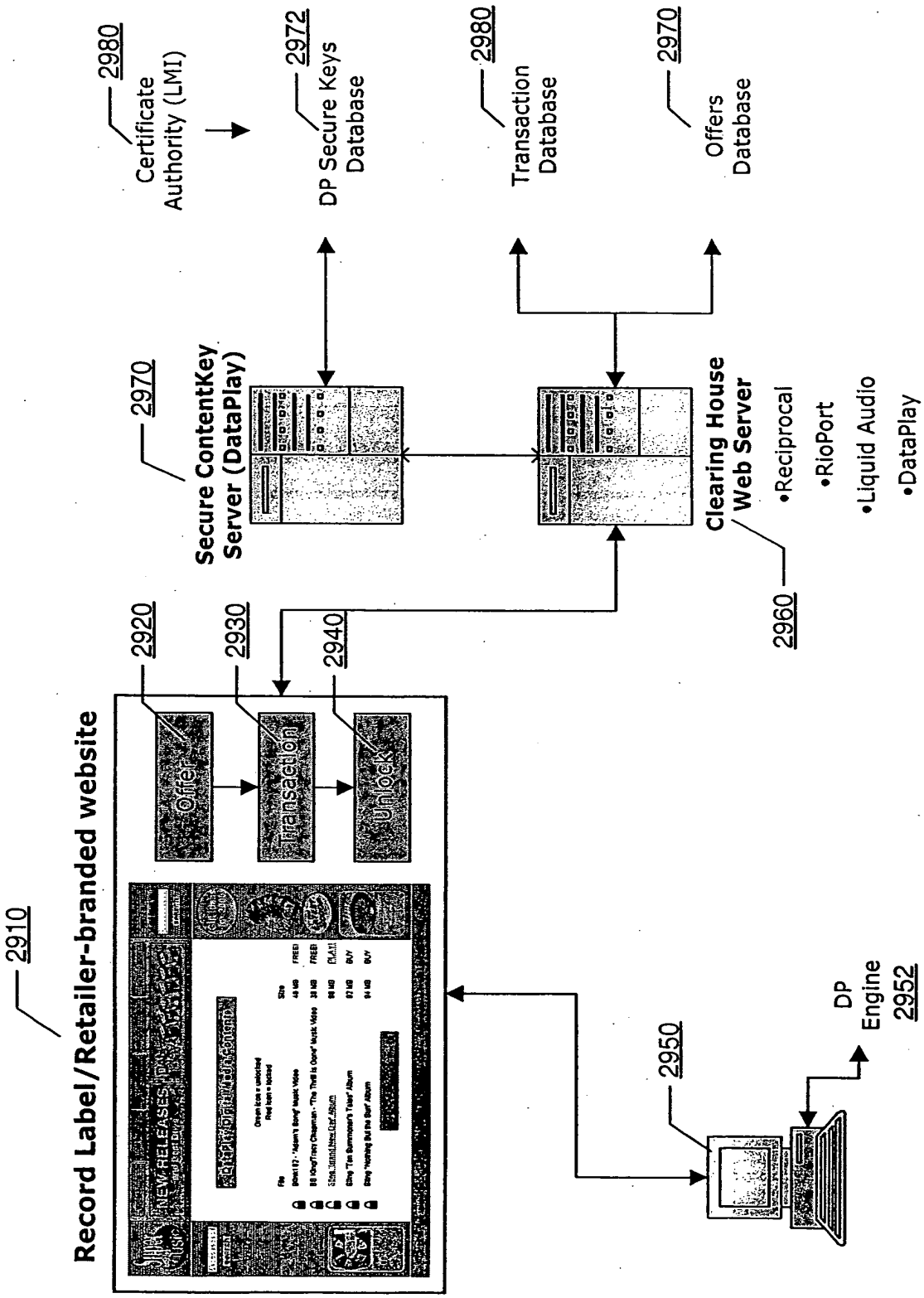


FIG. 29

TO/2180 - 9200660

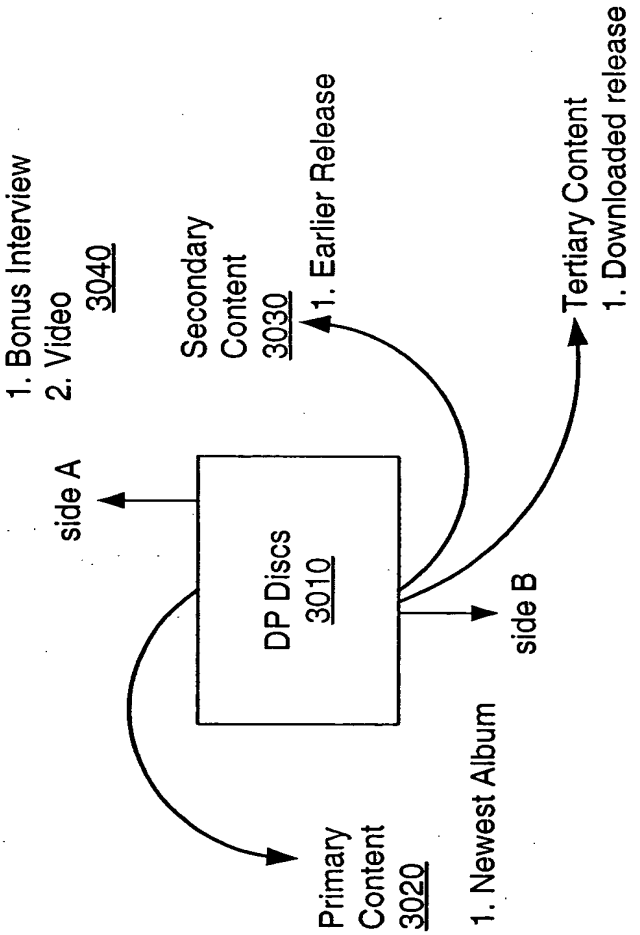

1. Bonus Interview
2. Video
3040
side A
DP Discs
3010
Secondary
Content
3030
1. Earlier Release
Tertiary Content
1. Downloaded release
side B
Primary
Content
3020
1. Newest Album

FIG. 30

TO280 "9200h660

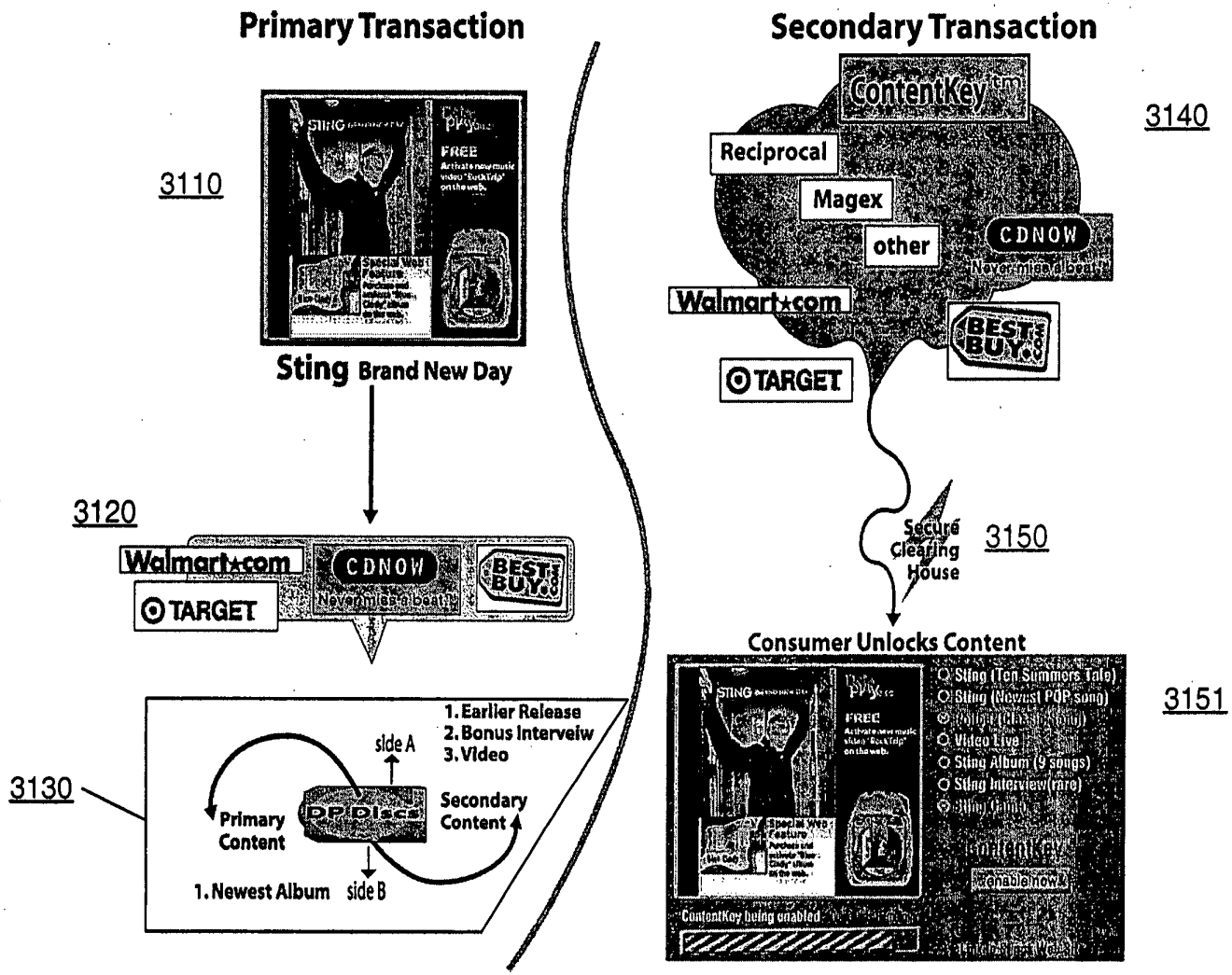


FIG. 31A

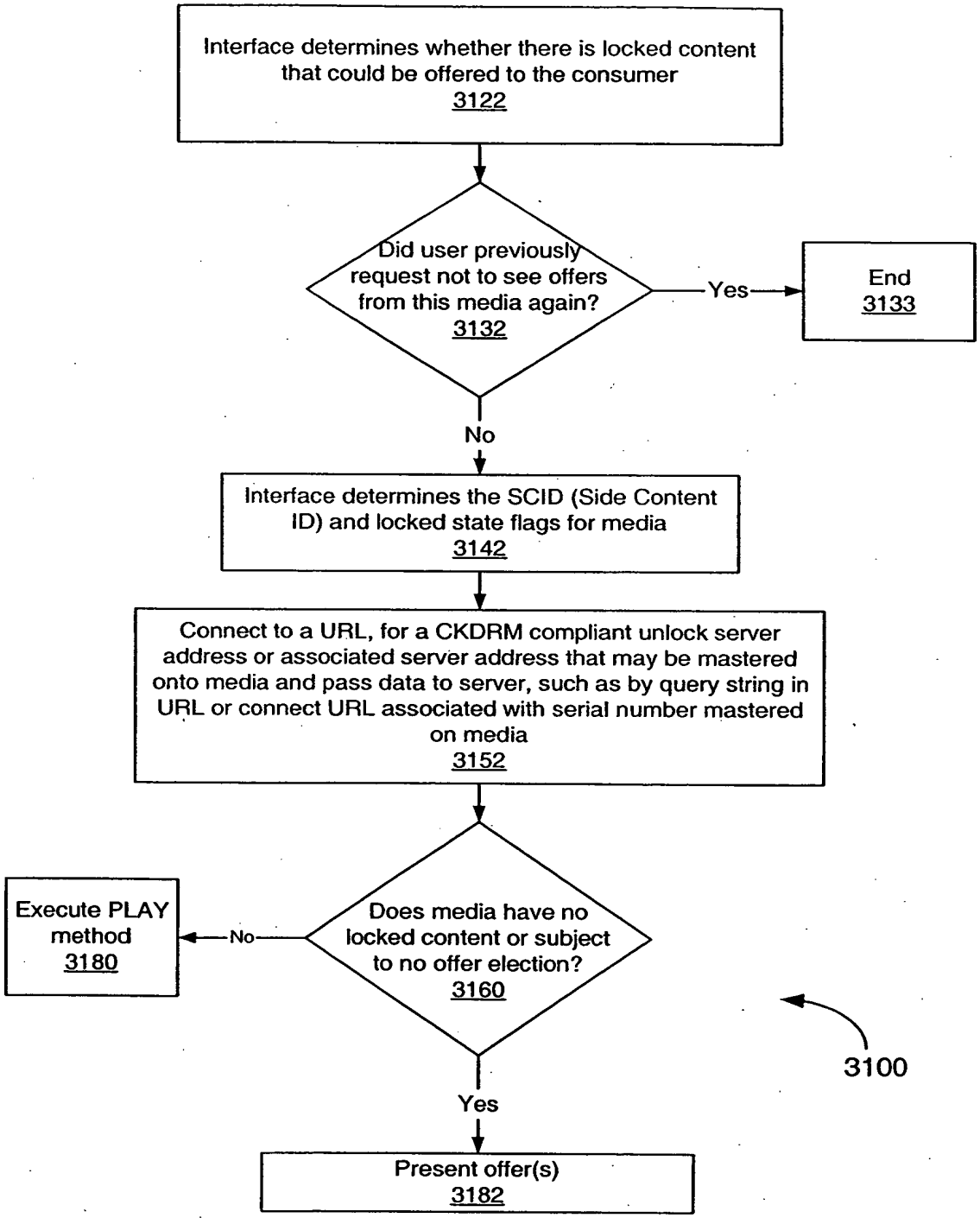

Interface determines whether there is locked content that could be offered to the consumer
3122
Did user previously request not to see offers from this media again?
3132
Yes
End
3133
No
Interface determines the SCID (Side Content ID) and locked state flags for media
3142
Connect to a URL, for a CKDRM compliant unlock server address or associated server address that may be mastered onto media and pass data to server, such as by query string in URL or connect URL associated with serial number mastered on media
3152
Does media have no locked content or subject to no offer election?
3160
No
Execute PLAY method
3180
Yes
Present offer(s)
3182
3100

FIG. 31B

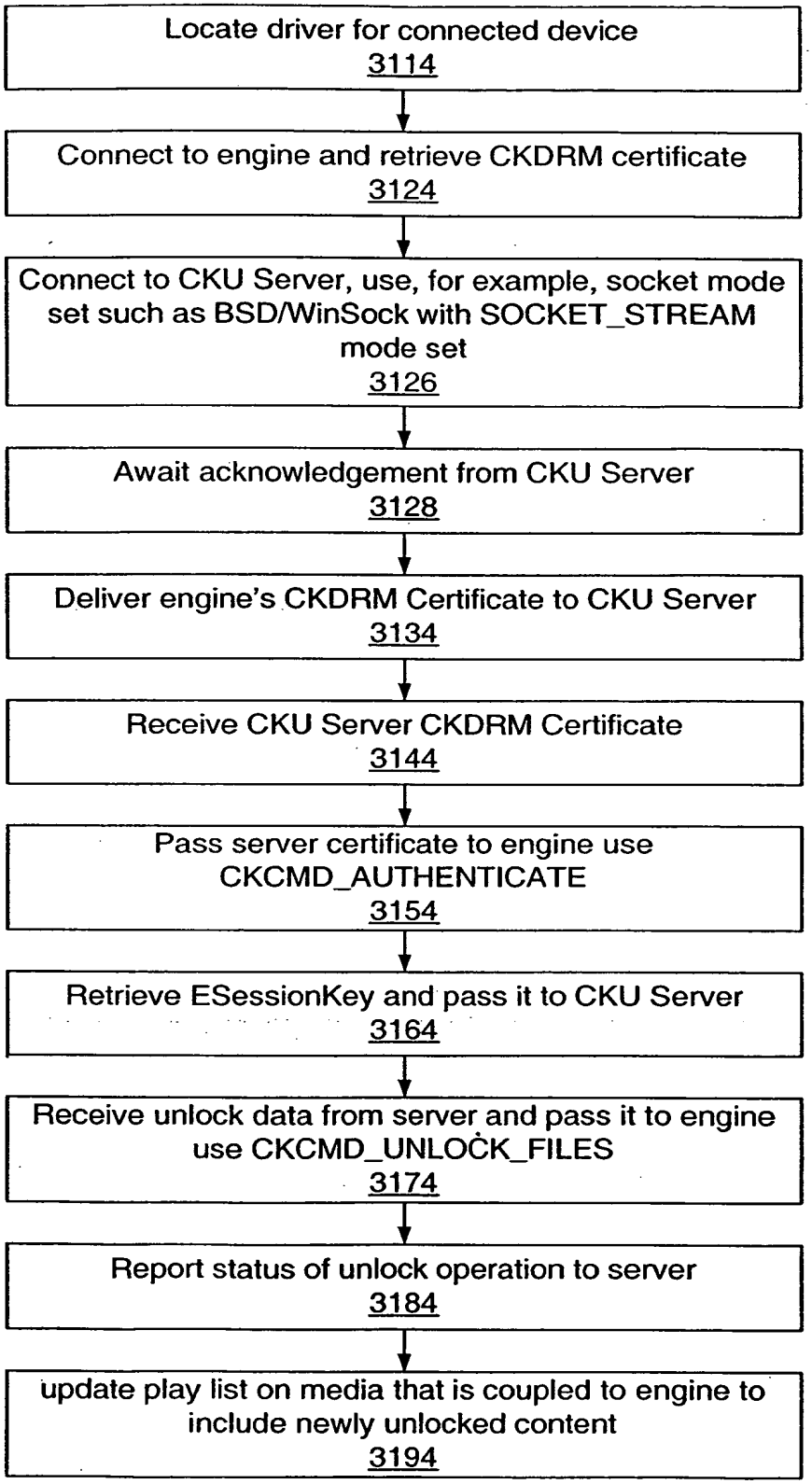

Locate driver for connected device
3114
Connect to engine and retrieve CKDRM certificate
3124
Connect to CKU Server, use, for example, socket mode set such as BSD/WinSock with SOCKET_STREAM mode set
3126
Await acknowledgement from CKU Server
3128
Deliver engine's CKDRM Certificate to CKU Server
3134
Receive CKU Server CKDRM Certificate
3144
Pass server certificate to engine use CKCMD_AUTHENTICATE
3154
Retrieve ESessionKey and pass it to CKU Server
3164
Receive unlock data from server and pass it to engine use CKCMD_UNLOCK_FILES
3174
Report status of unlock operation to server
3184
update play list on media that is coupled to engine to include newly unlocked content
3194

FIG. 31C

Attorney Docket No.: M-12041 US
First Inventor: Lane W. Lee
Title: Host Certification Method and System

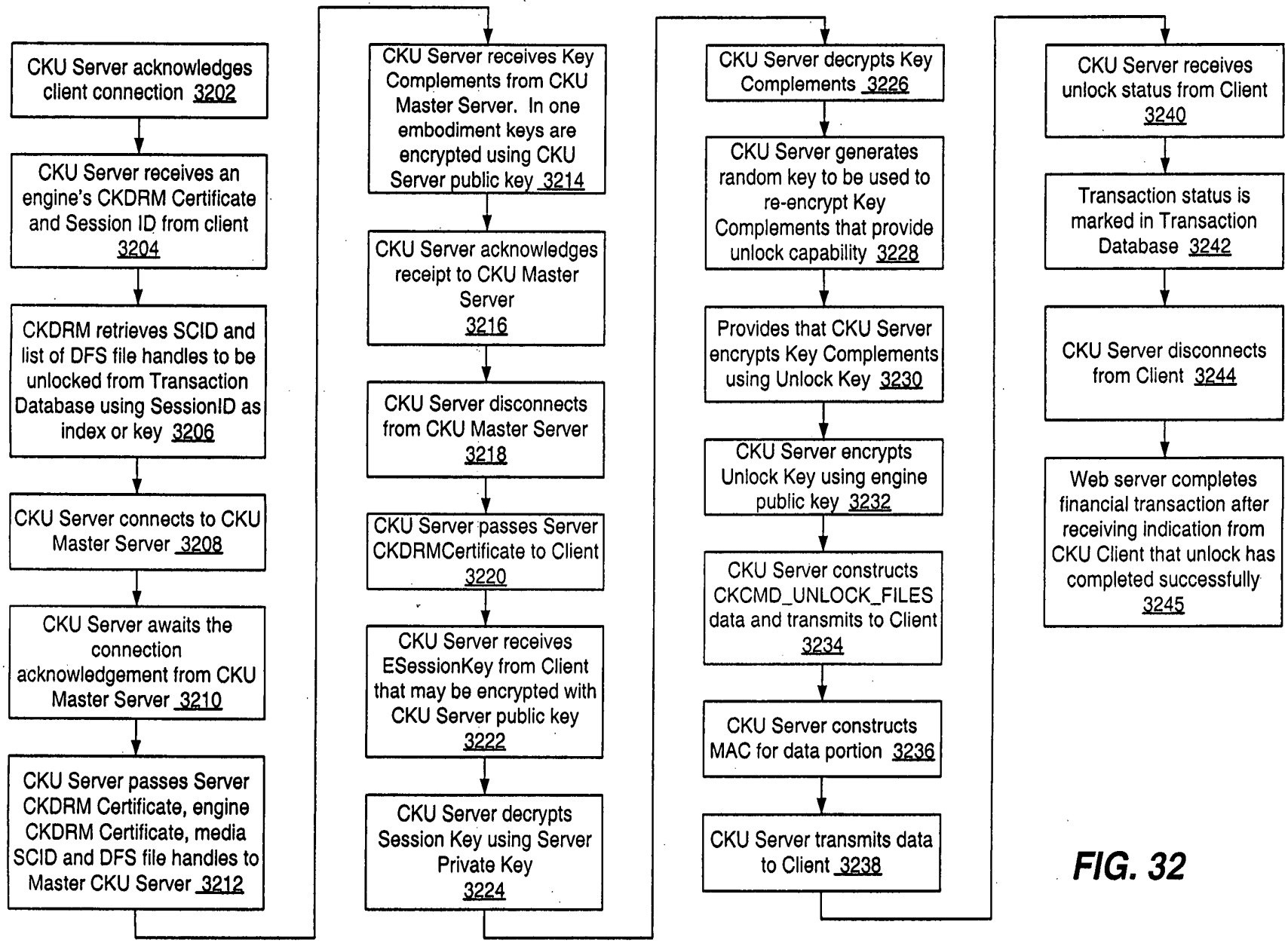


FIG. 32

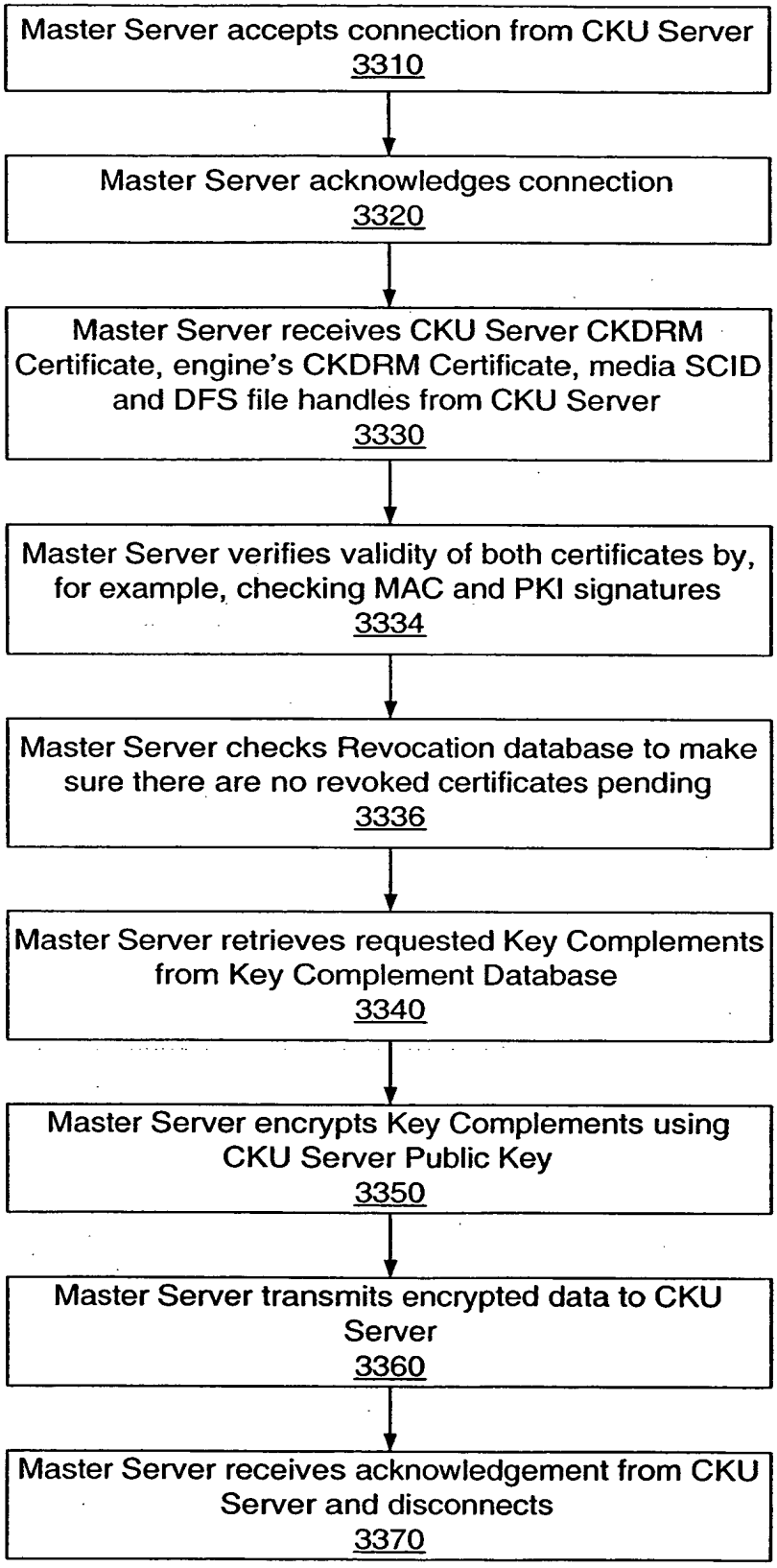


FIG. 33

P-12041-US

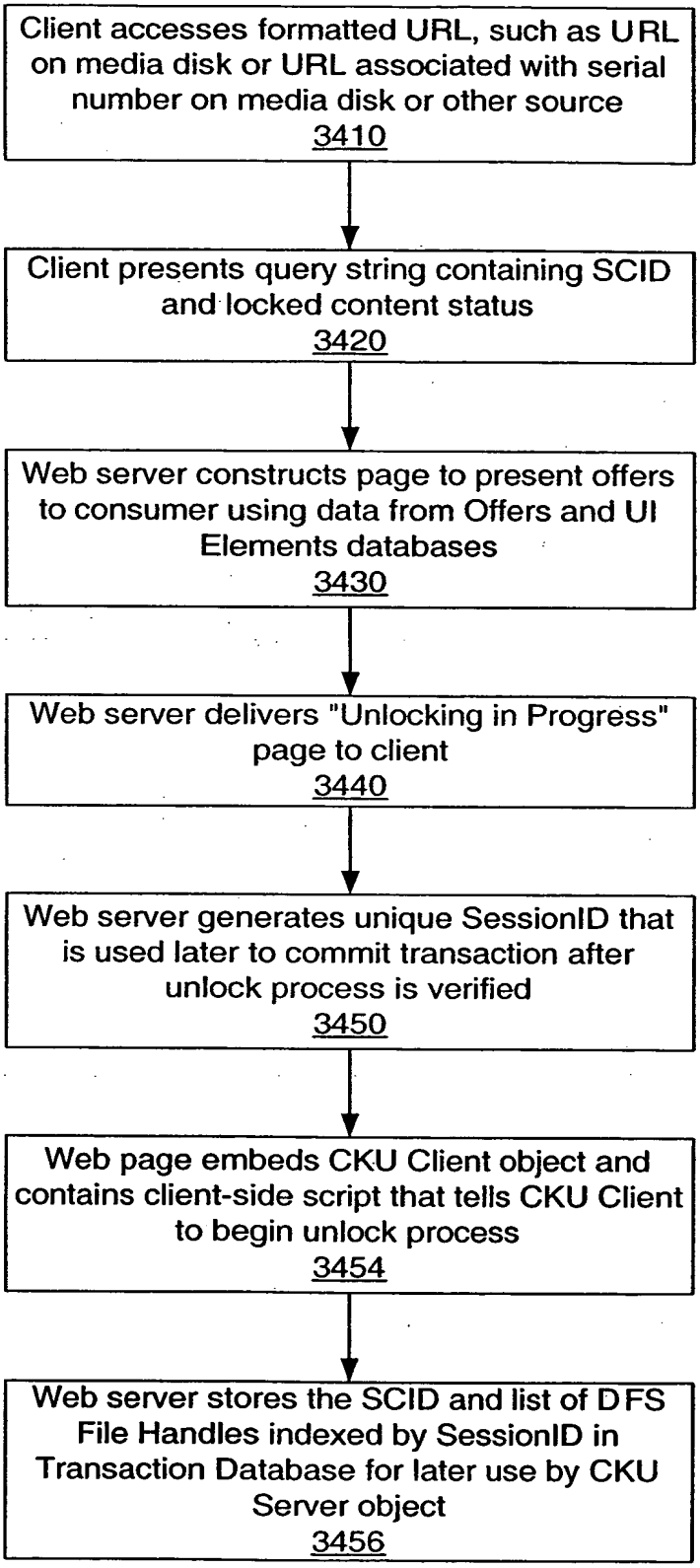


FIG. 34

0945026.08270.1

TO2280 "9200h660

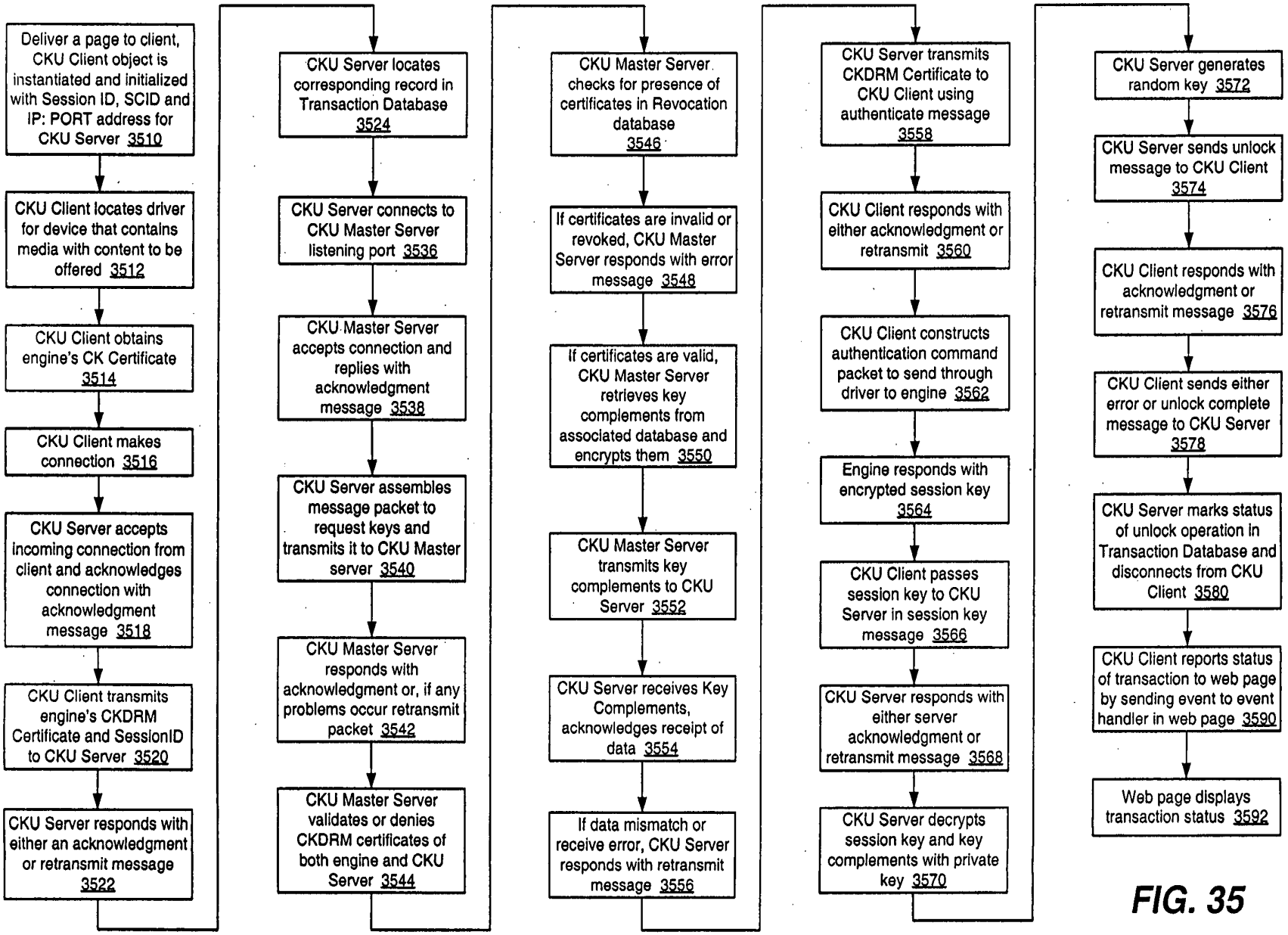


FIG. 35

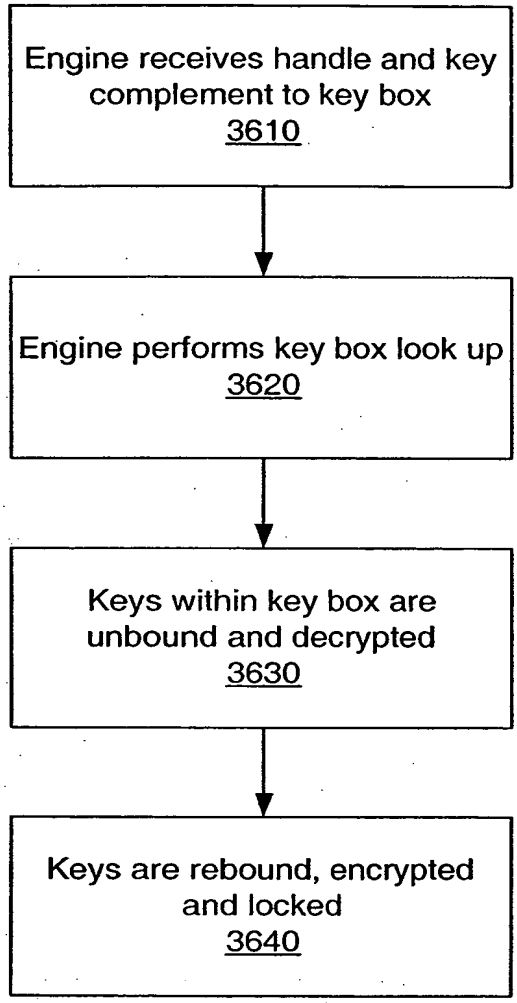


FIG. 36

Docket No. M-12041 US

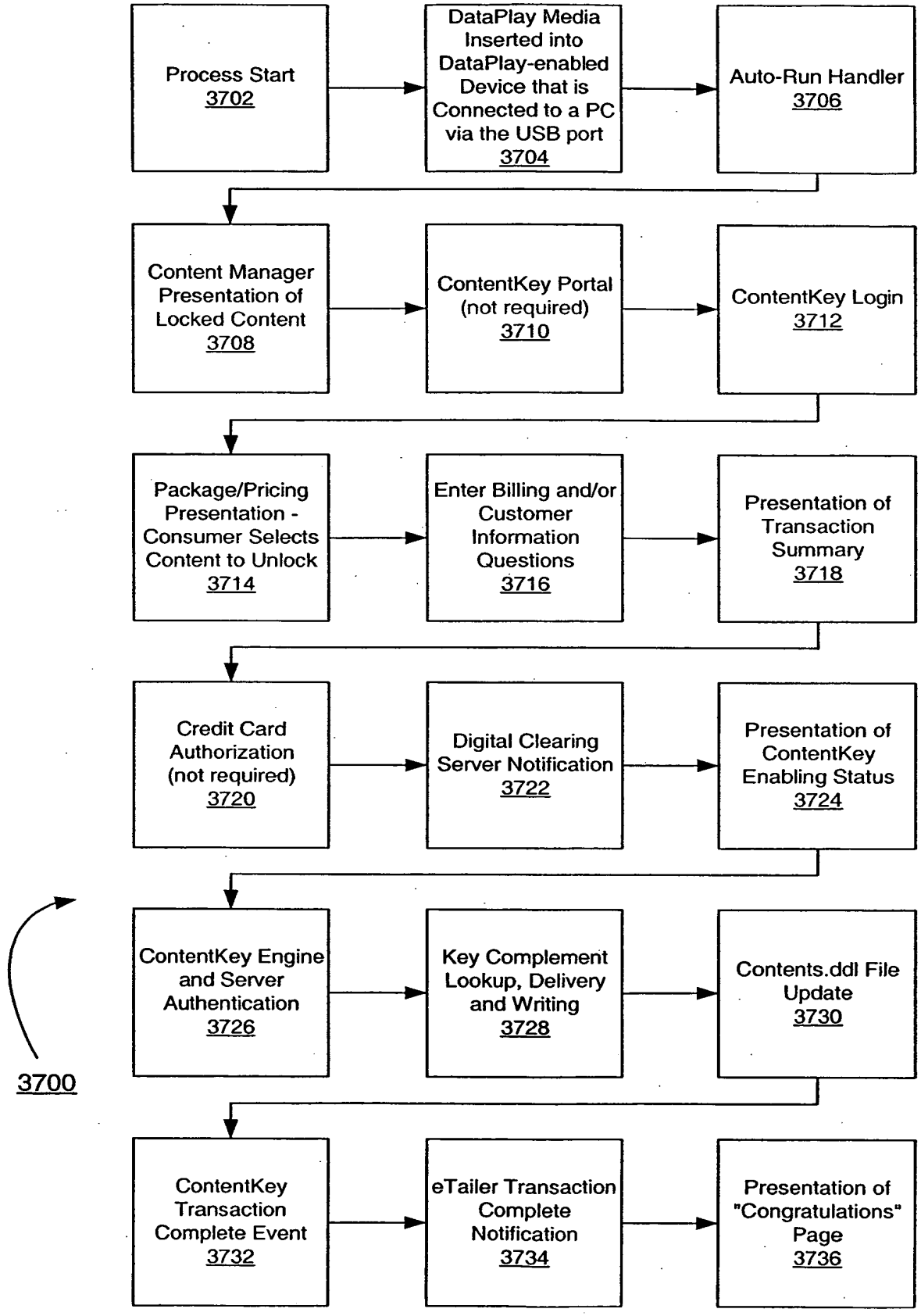


FIG. 37

EDCS-2300-0250

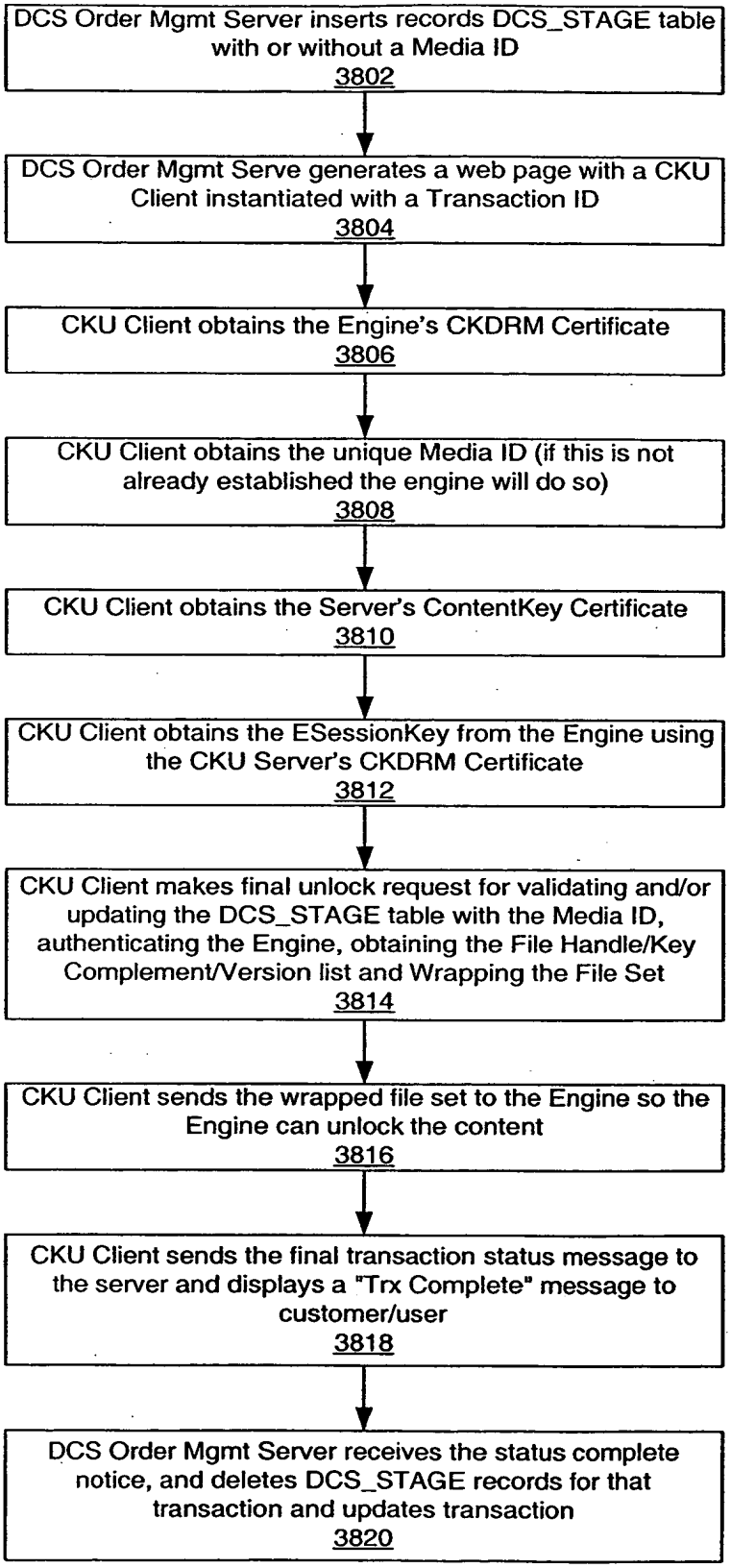


FIG. 38

05450026.082704

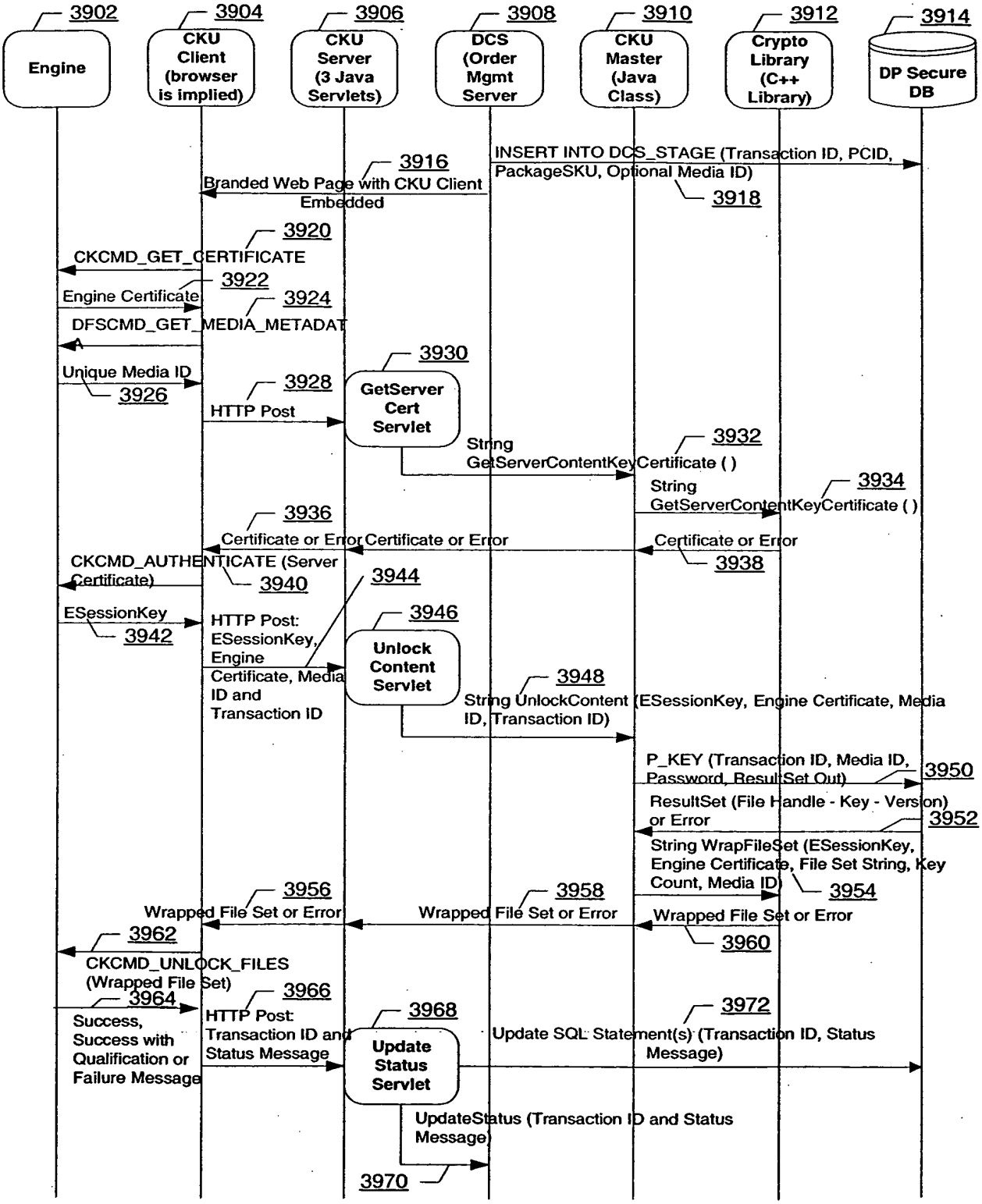


FIG. 39

Express Mail Label No. EV 339 450 150 US

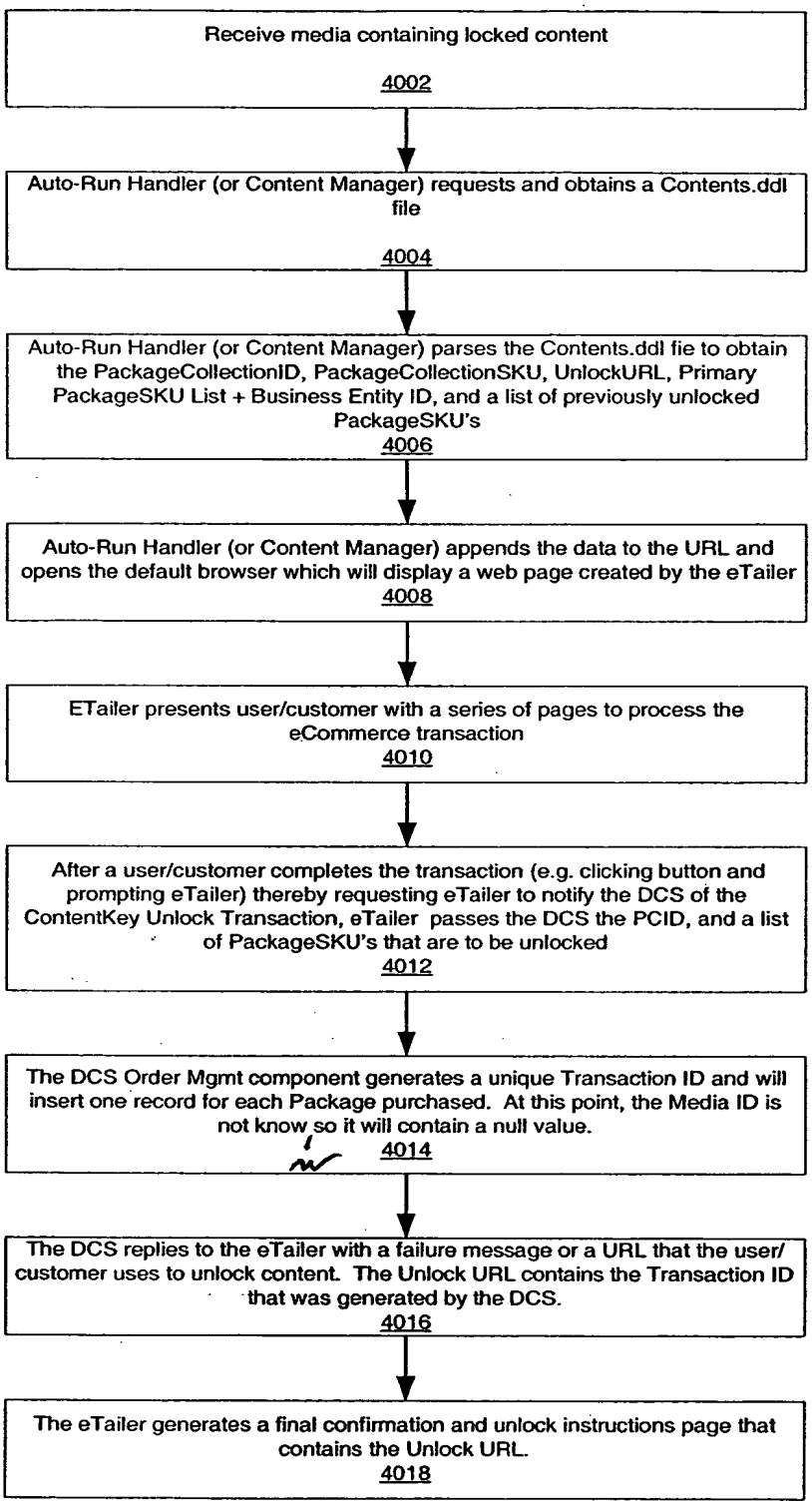

Receive media containing locked content
4002
Auto-Run Handler (or Content Manager) requests and obtains a Contents.ddl file
4004
Auto-Run Handler (or Content Manager) parses the Contents.ddl fie to obtain the PackageCollectionID, PackageCollectionSKU, UnlockURL, Primary PackageSKU List + Business Entity ID, and a list of previously unlocked PackageSKU's
4006
Auto-Run Handler (or Content Manager) appends the data to the URL and opens the default browser which will display a web page created by the eTailer
4008
ETailer presents user/customer with a series of pages to process the eCommerce transaction
4010
After a user/customer completes the transaction (e.g. clicking button and prompting eTailer) thereby requesting eTailer to notify the DCS of the ContentKey Unlock Transaction, eTailer passes the DCS the PCID, and a list of PackageSKU's that are to be unlocked
4012
The DCS Order Mgmt component generates a unique Transaction ID and will insert one record for each Package purchased. At this point, the Media ID is not know so it will contain a null value.
4014
The DCS replies to the eTailer with a failure message or a URL that the user/ customer uses to unlock content. The Unlock URL contains the Transaction ID that was generated by the DCS.
4016
The eTailer generates a final confirmation and unlock instructions page that contains the Unlock URL.
4018

FIG. 40

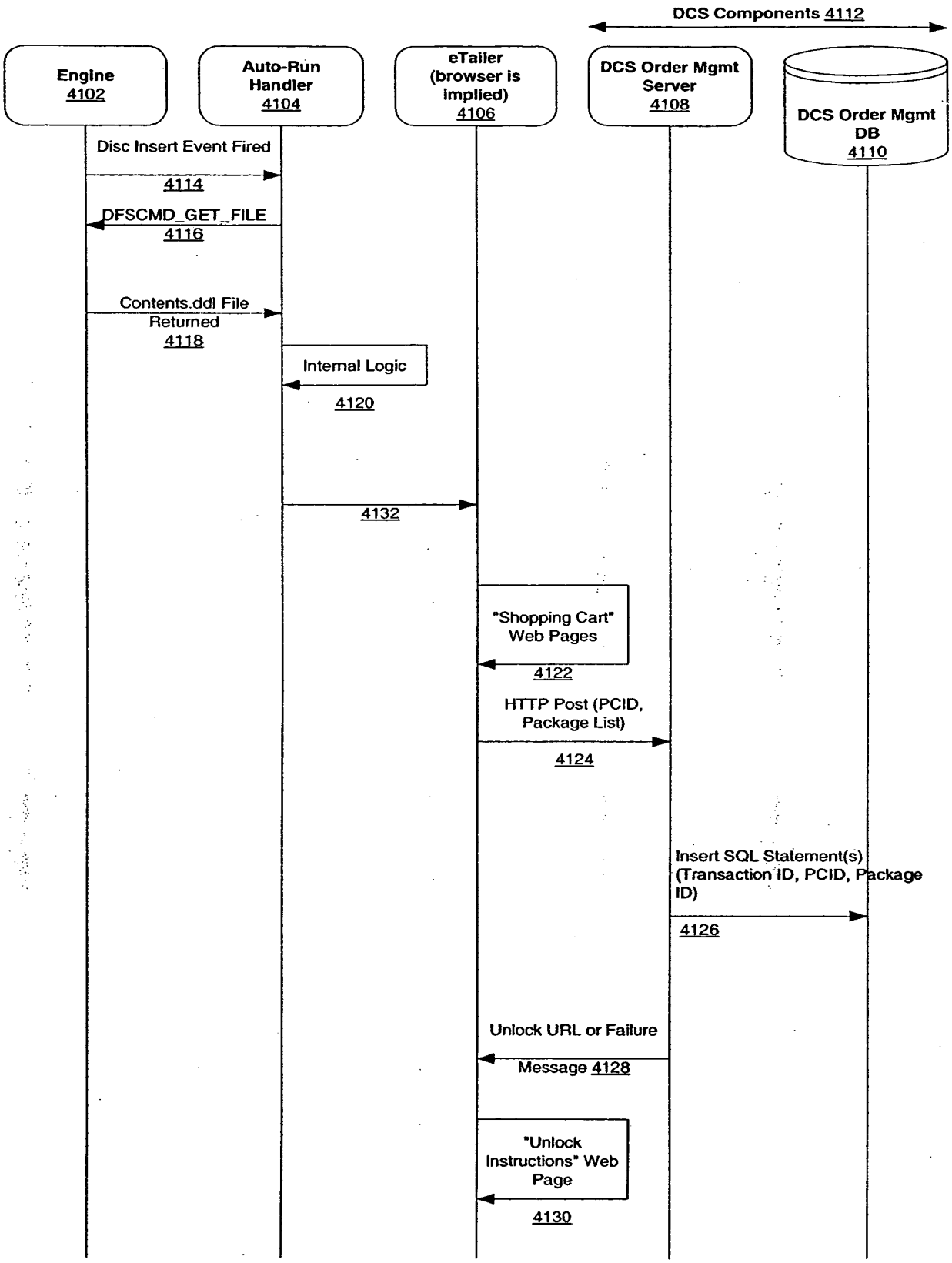

DCS Components 4112
Engine 4102
Auto-Run Handler 4104
eTailer (browser is implied) 4106
DCS Order Mgmt Server 4108
DCS Order Mgmt DB 4110
Disc Insert Event Fired
4114
DFSCMD_GET_FILE
4116
Contents.ddl File Returned
4118
Internal Logic
4120
4132
"Shopping Cart" Web Pages
4122
HTTP Post (PCID, Package List)
4124
Insert SQL Statement(s) (Transaction ID, PCID, Package ID)
4126
Unlock URL or Failure Message 4128
"Unlock Instructions" Web Page
4130

FIG. 41